document addendum

HP StorageWorks Fabric OS 3.x

First Edition (January 2005)

Part Number: AA–RW24A–TE

This document is an addendum for Fabric OS users to supplement the Fabric OS version 3.x documentation set. This document is specific to Fabric OS version 3.x and all switches running Fabric OS version 3.x, including the HP StorageWorks SAN Switch 2/8 EL, SAN Switch 2/16, and MSA SAN Switch 2/8.

invent

© Copyright 2004 Hewlett-Packard Development Company, L.P.

© Copyright 2004 Brocade Communications Systems, Incorporated.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Linux® is a U. S. registered trademark of Linus Torvlads.

Java^{TM} is a U. S. trademark of Sun Microsystems, Inc.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

Fabric OS 3.x Document Addendum
First Edition (January 2005)
Part Number: AA–RW24A–TE

contents

Figures

Tables

about this guide

This Addendum captures all documentation updates since the last release of the 3.x documentation set, for the following HP StorageWorks switches:

- HP StorageWorks SAN Switch 2/8 EL
- HP StorageWorks SAN Switch 2/16
- HP StorageWorks MSA SAN Switch 2/8

For example, this document provides important technical updates to the following documents:

- *HP StorageWorks Advanced Performance Monitor Version 3.1.x/4.1.x User Guide*, part number AA-RTS4C-TE
- *HP StorageWorks Web Tools Version 3.1.x/4.1.x User Guide*, part number AA-RS25C-TE
- *HP StorageWorks Zoning Version 3.1.x/4.1.x User Guide*, part number AA-RS26C-TE
- *HP StorageWorks Diagnostic And System Error Messages Version 3.1.x Reference Guide*, part number AA-RUPZA-TE
- *HP StorageWorks Extended Fabric Version 3.1.x/4.1.x User Guide*, part number AA-RTSDC-TE
- *HP StorageWorks Fabric Os Procedures Version 3.1.x/4.1.x User Guide*, part number AA-RS23C-TE
- *HP StorageWorks ISL Trunking Version 3.1.x/4.1.x User Guide*, part number AA-RTSAC-TE
- *HP StorageWorks Fabric Os Version 3.1.x/4.1.x Reference Guide*, part number AA-RS24C-TE
- *HP StorageWorks Fabric Watch Version 3.1.x/4.1.x User Guide*, part number AA-RTSGC-AA

Note: The technical updates provided in this Addendum apply if you are running Fabric OS 3.1.x or later.

This preface contains the following sections:

Overview

This section covers the following topics:

- Intended audience
- Related documentation

Intended audience

This book is intended for users of the Fabric OS version 3.1.x/4.1.x documentation set.

Related documentation

Related documents are listed on page 9. Documentation, including white papers and best practices documents, is available via the HP website. Please go to:

http://www.hp.com/country/us/eng/prodserv/storage.html

To access 4.x related documents:

1. Locate the **Networked storage** section of the web page.
2. Under **Networked storage**, go to the **By type** subsection.
3. Click **SAN infrastructure**. The SAN infrastructure page displays.
4. Locate the **Fibre Channel Switches** section.

   Locate the **B-Series Fabric** subsection, and then go to the **Entry Level** subsection.

   To access 3.x documents (such as this document), select the appropriate product, for example **SAN Switch 2/16, SAN Switch 2/8 EL, or MSA SAN Switch 2/8** models.

   The switch overview page displays.
5. Go to the **Product information** section, located on the far right side of the web page.
6. Click **Technical documents**.
7. Follow the on-screen instructions to download the applicable documents.

Conventions

Conventions consist of the following:

- Document conventions
- Text symbols

Document conventions

This document follows the conventions in Table 1.

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Key and field names, menu items, buttons, and dialog box names
Italics	File names, application names, and text emphasis
`Monospace font` `COMMAND NAMES` are uppercase monospace font unless they are case sensitive	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Variables
Blue underlined sans serif font text: http://www.hp.com	web site addresses

Text symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Getting help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP technical support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP storage web site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP authorized reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers: http://www.hp.com.

Advanced performance monitor user guide

1

This chapter contains updates to the *HP StorageWorks Advance Performance Monitor Version 3.1.x/4.1.x User Guide*, part number AA-RTS4C-TE.

On page 35, under the heading "Managing Performance Monitoring with Telnet Commands," replace the existing text with the following:

Telnet commands provide access to four different types of performance monitoring:

- AL_PA monitoring
- End-to-end monitoring
- Filter-based monitoring
- ISL monitoring (supported only in Fabric OS v3.2.x)

On page 37, immediately before the heading "Telnet Commands," add the following:

ISL Monitoring

Note: ISL monitoring is supported only in Fabric OS v3.2.x.

ISL monitoring measures the outbound traffic going through an ISL on the domain level. Using the information gathered, you can identify how the ISLs are used over a long period of time.

On page 37, at the end of Chapter 3, add the following:

Using ISL Monitoring

Note: ISL monitoring is supported only in Fabric OS v3.2.x.

ISL monitoring measures the amount of traffic each destination domain contributes to the overall traffic. If ISL monitors exceed 16 domains on a single trunk, approximate values are estimated. An ISL is considered a single entity even if it is a trunk or a single E_Port. If a trunk is to be monitored, the master trunk port is used to identify the ISL. The ISL monitor is discontinued when the master trunk port goes offline.

ISL monitoring is enabled by default, except when using HP Fabric Manager, for which ISL monitoring must be enabled on a per-switch basis. For more information, refer to the *HP StorageWorks Fabric Manager User Guide*.

You can display existing ISL monitors using the `perfMonitorShow` command. You can clear ISL monitor counters using the `perfMonitorClear` command.

Displaying ISL Monitors

Use the `perfMonitorShow` command to display all the ISL-based monitors on a specified port. This command displays the following information:

- 64-bit cumulative ISL transmit counter
- 64-bit cumulative transmit counter for each individual domain
- Total number of domains being monitored
- Number of ports in the ISL

The following example displays ISL monitors on port 7. In the example, there is one port in the ISL. Sixteen domains are monitored because there are routes going to those domains through this ISL

```
switch:admin> perfmonitorshow "ISL", 7

     Total transmit count for this ISL:       21748 g  780204495
     Number of destination domains monitored: 16
     Number of ports in this ISL: 1
     Domain  84:                        0      Domain  88:                 0
     Domain  89:                        0      Domain  90:                 0
     Domain  91:                        0      Domain  92:                 0
     Domain  95:       21748 g  780182720      Domain  96:               104
     Domain 100:                       36      Domain 102:                 0
     Domain 105:                        0      Domain 110:                 0
     Domain  80:                      112      Domain  81:             21299
     Domain  82:                      112      Domain  83:               112
```

Clearing ISL Monitors

Use the `perfMonitorClear` command to clear ISL monitor counters.

The following example clears statistical counters for an ISL monitor.

```
switch:admin> perfmonitorclear "ISL", 0
     This will clear ISL monitor on port 0, continue? (yes, y, no, n): [no] y
     ISL monitor on port 0 is cleared
```

Advanced Web Tools user guide

2

This chapter contains updates to the *HP StorageWorks Web Tools Version 3.1.x/4.1.x User Guide*, part number AA-RS25C-TE.

On original page 28, under the heading "Fabric Tree," after the following text:

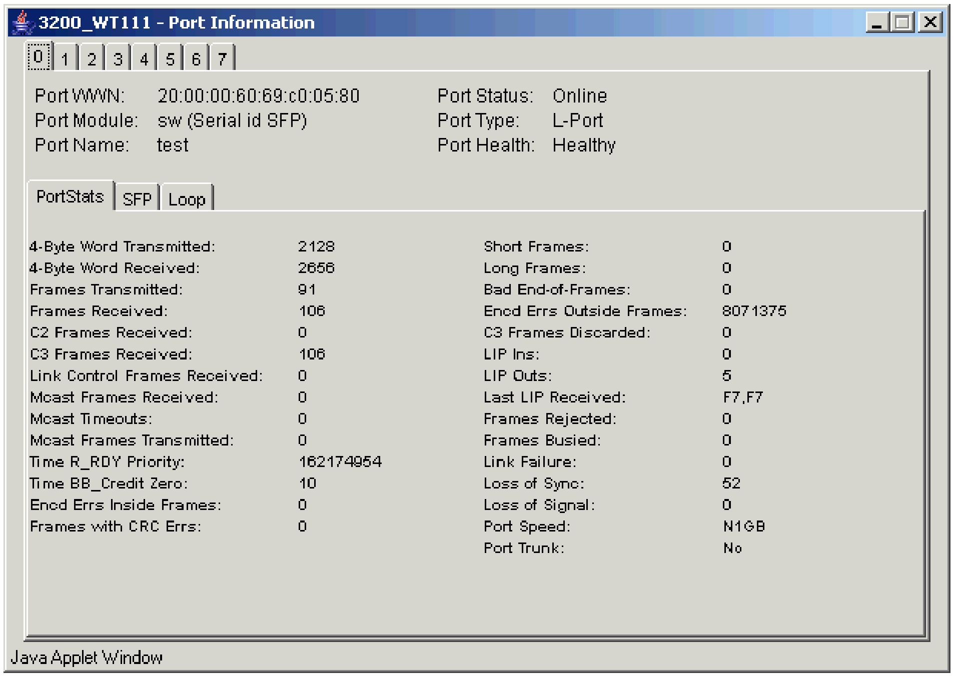
- A Fabric Admin tool bar which provides access to fabric level administration functionality including: Fabric Events, Topology, Name Server, and Zoning Admin.

Add this text:

The Fabric Tree status is updated at different time intervals, depending on the number of switches in the fabric. On average, for a fabric with up to 12 switches, the Fabric Tree status is updated every 30 seconds. For every additional 12 switches in the fabric, an additional 30 seconds is required to update the Fabric Tree status. The Switch Information View displays the last time the Fabric Tree status was updated.

You can also manually refresh the status of a switch within the fabric by right-clicking the name of that switch in the Fabric Tree and selecting **Refresh**. The Switch Information View displays the **Polled At** field, which identifies the last time the information was updated.

On original page 33, under the heading “Port Information View,” replace original Figure 5, “Port information view,” with the following:



```
Port WWN:     20:00:00:60:69:c0:05:80          Port Status:   Online
Port Module:  sw (Serial id SFP)               Port Type:     L-Port
Port Name:    test                             Port Health:   Healthy

4-Byte Word Transmitted:        2128           Short Frames:                 0
4-Byte Word Received:           2656           Long Frames:                  0
Frames Transmitted:             91             Bad End-of-Frames:            0
Frames Received:                106            Encd Errs Outside Frames:     8071375
C2 Frames Received:             0              C3 Frames Discarded:          0
C3 Frames Received:             106            LIP Ins:                      0
Link Control Frames Received:   0              LIP Outs:                     5
Mcast Frames Received:          0              Last LIP Received:            F7,F7
Mcast Timeouts:                 0              Frames Rejected:              0
Mcast Frames Transmitted:       0              Frames Busied:                0
Time R_RDY Priority:            162174954      Link Failure:                 0
Time BB_Credit Zero:            10             Loss of Sync:                 52
Encd Errs Inside Frames:        0              Loss of Signal:               0
Frames with CRC Errs:           0              Port Speed:                   N1GB
                                               Port Trunk:                   No
```

Figure 1: Port information view

On original pages 36 and 37, replace the entire “Workstation Requirements” section with the following:

Table 2 identifies the supported browsers, operating systems, and Java™ Plug-ins for this release.

Table 2: Supported platforms

Operating system	Browser	Java plug-in
RedHat Linux® 9.0	Mozilla 1.6	1.4.2_03
Solaris 2.8	Mozilla 1.6	1.4.2_03
Solaris 2.9	Mozilla 1.6	1.4.2_03
Windows® 2000	Internet Explorer 6.0	1.4.2_03
Windows 2003	Internet Explorer 6.0	1.4.2_03
Windows XP	Internet Explorer 6.0	1.4.2_03

Adequate RAM is required on Windows systems as follows:

- 128 MB or more RAM for fabrics comprising 10 switches or fewer
- 256 MB or more RAM for fabrics comprising 15 switches or fewer
- 512 MB or more RAM for fabrics comprising more than 15 switches

A minimum of 8 MB of video RAM is also recommended.

On original page 38, replace the entire “Installing a Web Browser” section with the following:

If not already installed, install one of the following browsers:

- Internet Explorer 6.0
- Mozilla 1.6

For instructions on installing Mozilla 1.6 on Solaris 2.8 and Solaris 2.9, refer to the following web site:

http://ftp27f.newaol.com/pub/mozilla.org/mozilla/releases/mozilla1.6/README

Note: This URL is subject to change without notice.

On original pages 38 and 39, replace the entire “Configuring the Web Browser” section with the following:

Configuring the Web Browser

Specific browser settings are required for the correct operation of Web Tools with Internet Explorer or Mozilla (supported on Solaris only).

Configuring Internet Explorer

Correct operation of Web Tools with Internet Explorer requires specifying the appropriate settings for browser refresh frequency. Browser pages should be refreshed frequently to ensure the correct operation of Web Tools.

To set the refresh frequency:

1. Select **Preferences** from the **Edit** menu.
2. Select the **General** tab and click **Settings** (under **Temporary Internet Files**).
3. Under **Check for newer versions of stored pages,** select **Every visit to the page**.

Configuring Mozilla

Some browsers use local cache copies of `.jar` files and image files to improve performance (depending on the options selected in the browser), which can cause incorrect displays in Web Tools. The Web browser cache must be cleared before invoking Web Tools.

To clear the cache and set the refresh frequency:

1. Select **Edit** > **Preferences**.
2. Click **Advanced** in the Category box to expand it and then click **Cache**.
3. On the Cache panel, click **Clear Cache**.
4. Under **Compare the page in the cache to the page on the network**, select **Every time I view the page**.
5. Click **OK**.

On original page 40, replace the following text:

Installing the Java Plug-in on Windows XP, 2000, or NT

To determine the version of the Java Plug-in installed on Windows XP, NT, or 2000, and install if necessary:

With the this text:

Installing the Java Plug-in on Windows XP, 2000, or 2003

To determine the version of the Java Plug-in installed on Windows XP, 2000, or 2003, and install if necessary:

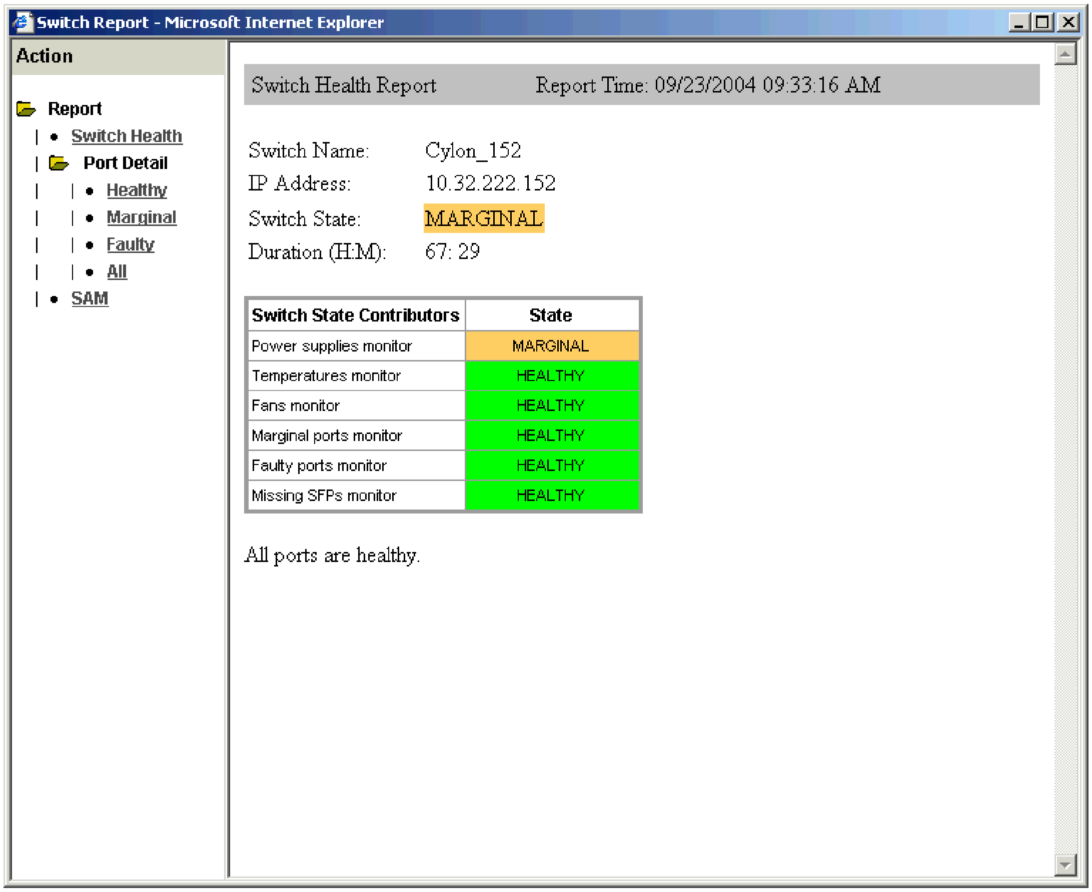
On original page 41, under the heading "Licensing Web Tools on the Switch," add the following heading and text:

Two and Four Domain Fabric Licensing

If your fabric includes a switch with a license for a limited number of switches in the fabric and the fabric exceeds the switch limit indicated in the license, Web Tools allows a 45-day grace period in which you can still monitor the switch.

Web Tools displays warning messages periodically, informing you that your fabric size exceeds the supported switch configuration limit and telling you how long you have before Web Tools will be disabled. After the 45-day grace period, you will no longer be able to launch Web Tools from the switch with the limited switch license, if that switch still exceeds the switch limit. Two domain/four domain fabric licensing is applicable only to 2 Gbps switches.

On original page 65, under the heading "Switch Status Example," replace original Figure 13, "Switch status window," with the following:



Switch Health Report Report Time: 09/23/2004 09:33:16 AM

Switch Name: Cylon_152
IP Address: 10.32.222.152
Switch State: MARGINAL
Duration (H:M): 67: 29

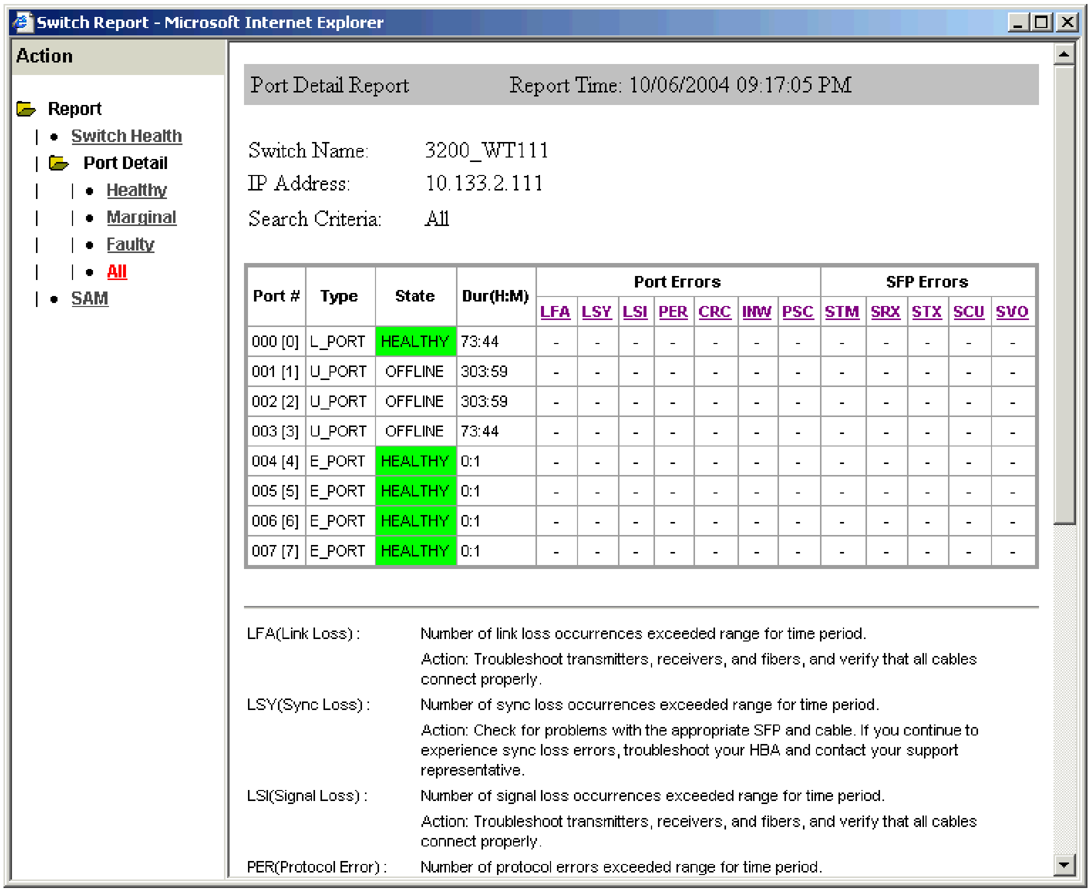
Switch State Contributors	State
Power supplies monitor	MARGINAL
Temperatures monitor	HEALTHY
Fans monitor	HEALTHY
Marginal ports monitor	HEALTHY
Faulty ports monitor	HEALTHY
Missing SFPs monitor	HEALTHY

All ports are healthy.

Figure 2: Switch status window

On original page 66, under the heading "Using the Switch Status Button," add the following at the end of the procedure:

6. Optional: Click the underlined links in the left panel to display detailed information about ports and Switch Availability Monitoring (SAM). Figure 3 shows an example of the Port Detail report.
7. Optional: Mouse-over the Action field and click an action to:
   - Refresh the information displayed in the report
   - Customize the report
   - View the data in raw XML format
   - View the style sheet for the report
   - View the XML schema for the report



Port Detail Report   Report Time: 10/06/2004 09:17:05 PM

Switch Name: 3200_WT111
IP Address: 10.133.2.111
Search Criteria: All

Port #	Type	State	Dur(H:M)	Port Errors							SFP Errors				
				LFA	LSY	LSI	PER	CRC	INW	PSC	STM	SRX	STX	SCU	SVO
000 [0]	L_PORT	HEALTHY	73:44	-	-	-	-	-	-	-	-	-	-	-	-
001 [1]	U_PORT	OFFLINE	303:59	-	-	-	-	-	-	-	-	-	-	-	-
002 [2]	U_PORT	OFFLINE	303:59	-	-	-	-	-	-	-	-	-	-	-	-
003 [3]	U_PORT	OFFLINE	73:44	-	-	-	-	-	-	-	-	-	-	-	-
004 [4]	E_PORT	HEALTHY	0:1	-	-	-	-	-	-	-	-	-	-	-	-
005 [5]	E_PORT	HEALTHY	0:1	-	-	-	-	-	-	-	-	-	-	-	-
006 [6]	E_PORT	HEALTHY	0:1	-	-	-	-	-	-	-	-	-	-	-	-
007 [7]	E_PORT	HEALTHY	0:1	-	-	-	-	-	-	-	-	-	-	-	-

LFA(Link Loss) : Number of link loss occurrences exceeded range for time period.
Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.

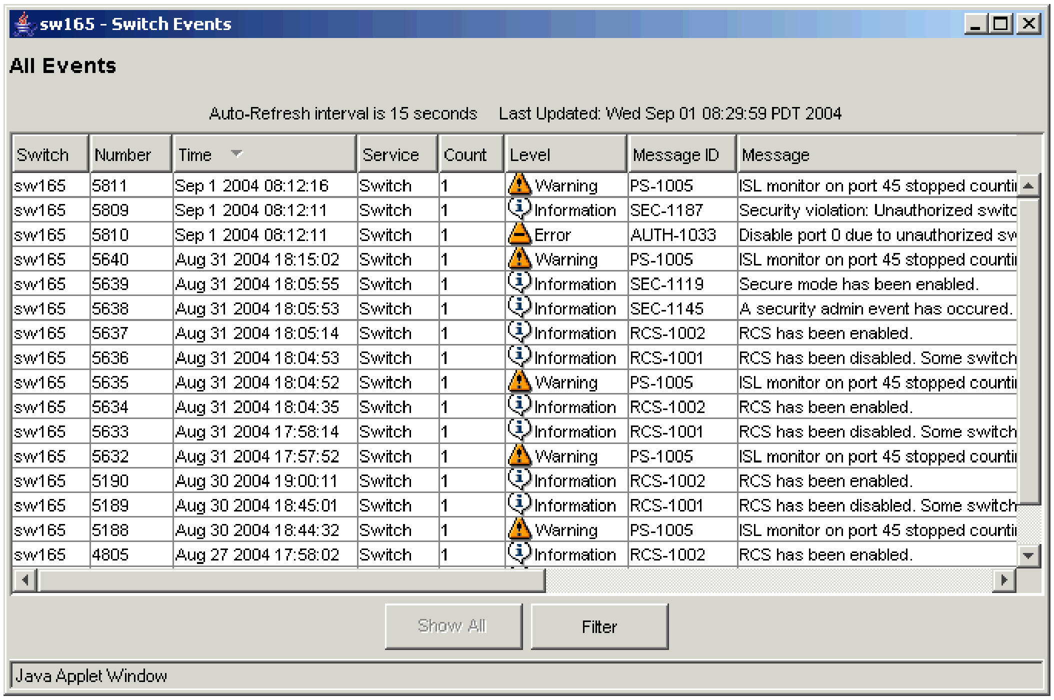
LSY(Sync Loss) : Number of sync loss occurrences exceeded range for time period.
Action: Check for problems with the appropriate SFP and cable. If you continue to experience sync loss errors, troubleshoot your HBA and contact your support representative.

LSI(Signal Loss) : Number of signal loss occurrences exceeded range for time period.
Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.

PER(Protocol Error) : Number of protocol errors exceeded range for time period.

Figure 3: Switch status window, port detail

On original page 67, under the heading "Switch Events Example," replace original Figure 14, "Switch events window," with the following:



All Events

Auto-Refresh interval is 15 seconds   Last Updated: Wed Sep 01 08:29:59 PDT 2004

Switch	Number	Time	Service	Count	Level	Message ID	Message
sw165	5811	Sep 1 2004 08:12:16	Switch	1	Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	5809	Sep 1 2004 08:12:11	Switch	1	Information	SEC-1187	Security violation: Unauthorized switc
sw165	5810	Sep 1 2004 08:12:11	Switch	1	Error	AUTH-1033	Disable port 0 due to unauthorized sw
sw165	5640	Aug 31 2004 18:15:02	Switch	1	Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	5639	Aug 31 2004 18:05:55	Switch	1	Information	SEC-1119	Secure mode has been enabled.
sw165	5638	Aug 31 2004 18:05:53	Switch	1	Information	SEC-1145	A security admin event has occured.
sw165	5637	Aug 31 2004 18:05:14	Switch	1	Information	RCS-1002	RCS has been enabled.
sw165	5636	Aug 31 2004 18:04:53	Switch	1	Information	RCS-1001	RCS has been disabled. Some switch
sw165	5635	Aug 31 2004 18:04:52	Switch	1	Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	5634	Aug 31 2004 18:04:35	Switch	1	Information	RCS-1002	RCS has been enabled.
sw165	5633	Aug 31 2004 17:58:14	Switch	1	Information	RCS-1001	RCS has been disabled. Some switch
sw165	5632	Aug 31 2004 17:57:52	Switch	1	Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	5190	Aug 30 2004 19:00:11	Switch	1	Information	RCS-1002	RCS has been enabled.
sw165	5189	Aug 30 2004 18:45:01	Switch	1	Information	RCS-1001	RCS has been disabled. Some switch
sw165	5188	Aug 30 2004 18:44:32	Switch	1	Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	4805	Aug 27 2004 17:58:02	Switch	1	Information	RCS-1002	RCS has been enabled.

Figure 4: Switch events window

On original page 67, under the heading "About the Switch Events Button," add the following:

Filtering Switch Events

You can filter the events in the Switch Events window by time and severity. You can apply just one type of filter at a time or all types of filters at the same time. Click the **Filter** button to display the Event Filter dialog box (Figure 5).

When a filter is applied, the Show All button is active in the Events Report and the types of filters applied are identified at the top of the Events Report. To un-apply a filter, click the **Show All** button in the Events Report.

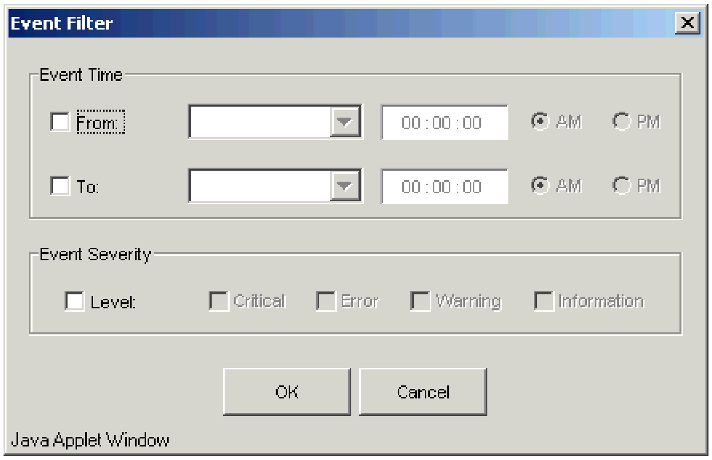


Figure 5: Event filter dialog box

Filtering Events by Time Intervals

To filter events by time intervals:

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree.

   The Switch View opens.
3. Select the **Switch Events** button from the Switch View.

   A Switch Events Report appears.
4. Click **Filter**.

   The Event Filter dialog box opens.
5. Optional: To filter events within a certain time period:
   a. Click **From** and enter the start time and date in the fields.
   b. Click **To** and enter the finish time and date in the fields.
6. Optional: To filter all events beginning at a certain date and time, click **From** and enter the start time and date in the fields.
7. Optional: To filter events up until a certain date and time, click **To** and enter the finish time and date in the fields.
8. Click **OK**.

   The filter is enabled and the enabled filter type is displayed in the Events Report.

Filtering Events by Event Severity

To filter events by event severity levels:

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree.

   The Switch View opens.

3. Select the **Switch Events** button from the Switch View.

   A Switch Events Report appears.
4. Click **Filter**.

   The Event Filter dialog box opens.
5. Click **Level**.

   The event severity level check boxes are enabled.
6. Select the event levels you want to display.
7. Click **OK**.

   The filter is enabled and the enabled filter type is displayed in the Events Report.

On original page 92, under the heading "Switch Admin Window Field Descriptions," modify original Table 17, "Switch Admin Window Field Descriptions," as follows.

Delete the following row:

Reset	Click this button to reset the field values to the last set of committed changes. If the Apply button has not been pressed on this tab, the parameters are returned to the original values the tab contained when it was initially displayed.

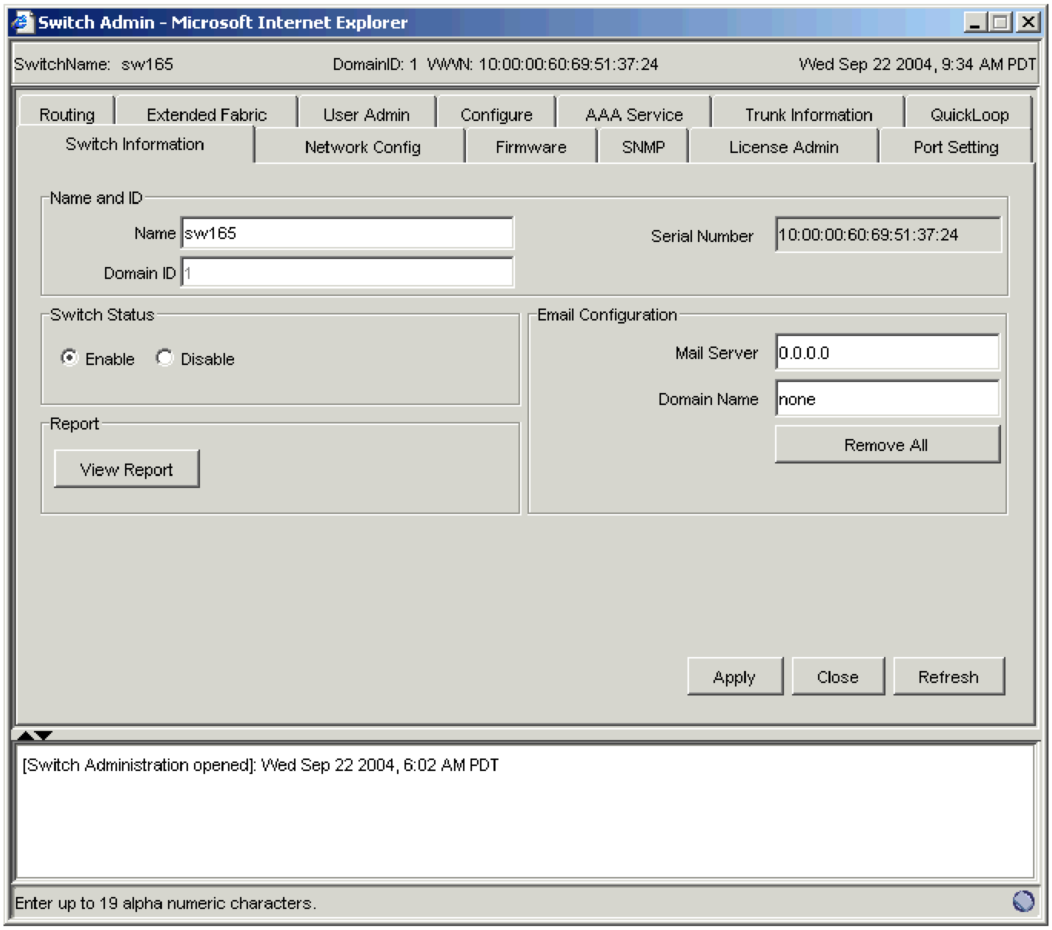
In the last row (Status Icon) in the table, replace the following text:

A green square means the switch is enabled; a red square means the switch is disabled.

With this text:

The ● icon means the switch is enabled, and the ⊘ icon means the switch is disabled.

On original page 95, under the heading “Switch Information Tab Example,” replace original Figure 18, “Switch Information Tab,” with the following:



Switch Admin - Microsoft Internet Explorer

SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 9:34 AM PDT

Name and ID

Name: sw165

Domain ID: 1

Serial Number: 10:00:00:60:69:51:37:24

Switch Status

● Enable ○ Disable

Email Configuration

Mail Server: 0.0.0.0

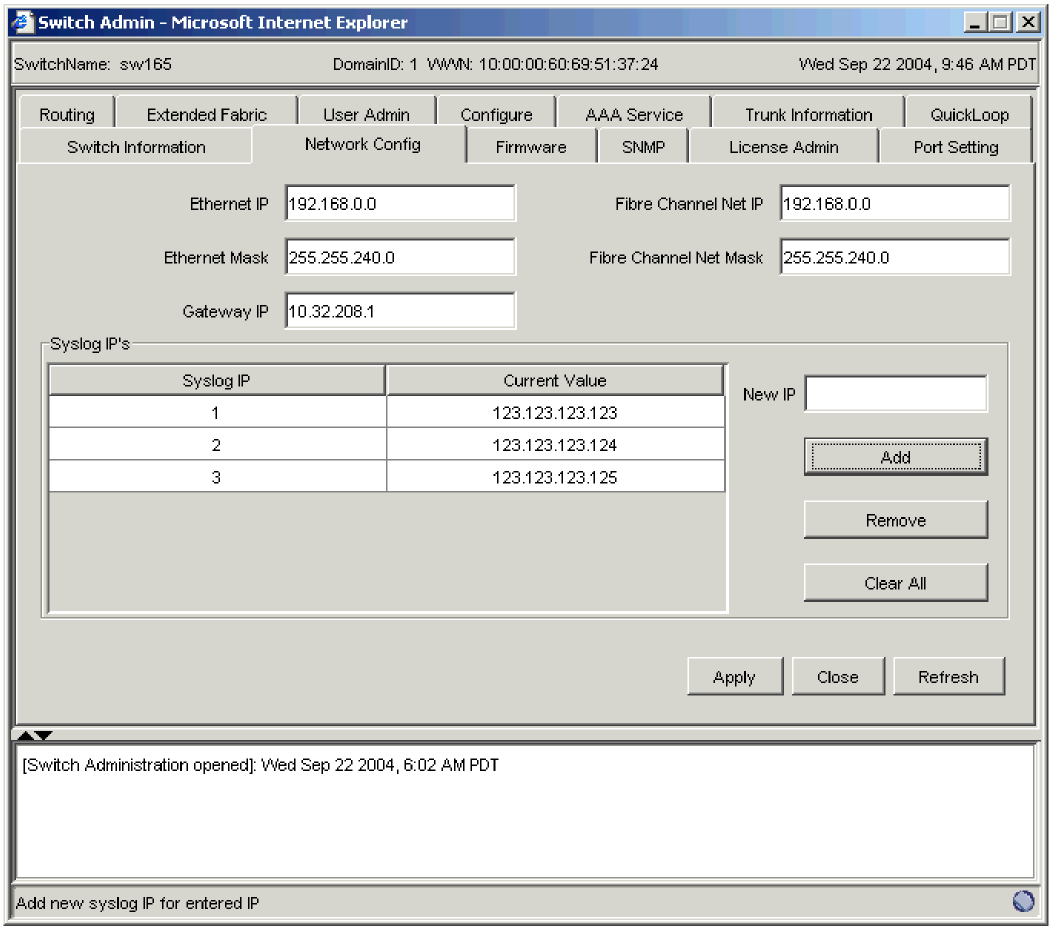
Domain Name: none

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Enter up to 19 alpha numeric characters.

Figure 6: Switch Information Tab

On original page 99, under the heading “Network Config Tab Example,” replace original Figure 19, “Network Configuration Tab,” with the following:



SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 9:46 AM PDT

Ethernet IP: 192.168.0.0

Ethernet Mask: 255.255.240.0

Gateway IP: 10.32.208.1

Fibre Channel Net IP: 192.168.0.0

Fibre Channel Net Mask: 255.255.240.0

Syslog IP	Current Value
1	123.123.123.123
2	123.123.123.124
3	123.123.123.125

New IP:

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Add new syslog IP for entered IP

Figure 7: Network Configuration Tab

On original page 100, in original Table 19, “Network Config Field Descriptions,” delete the following row:

Syslog IP Field	Enter any valid IP for a host and click the Add button to configure that IP as a recipient of syslog messages.

And replace it with this row:

New IP Field	Enter any valid IP for a host and click the Add button to configure that IP as a recipient of syslog messages.

On original pages 103 through 105, replace the entire section, “About the Upload/Download Tab,” with the following:

About the Firmware Tab

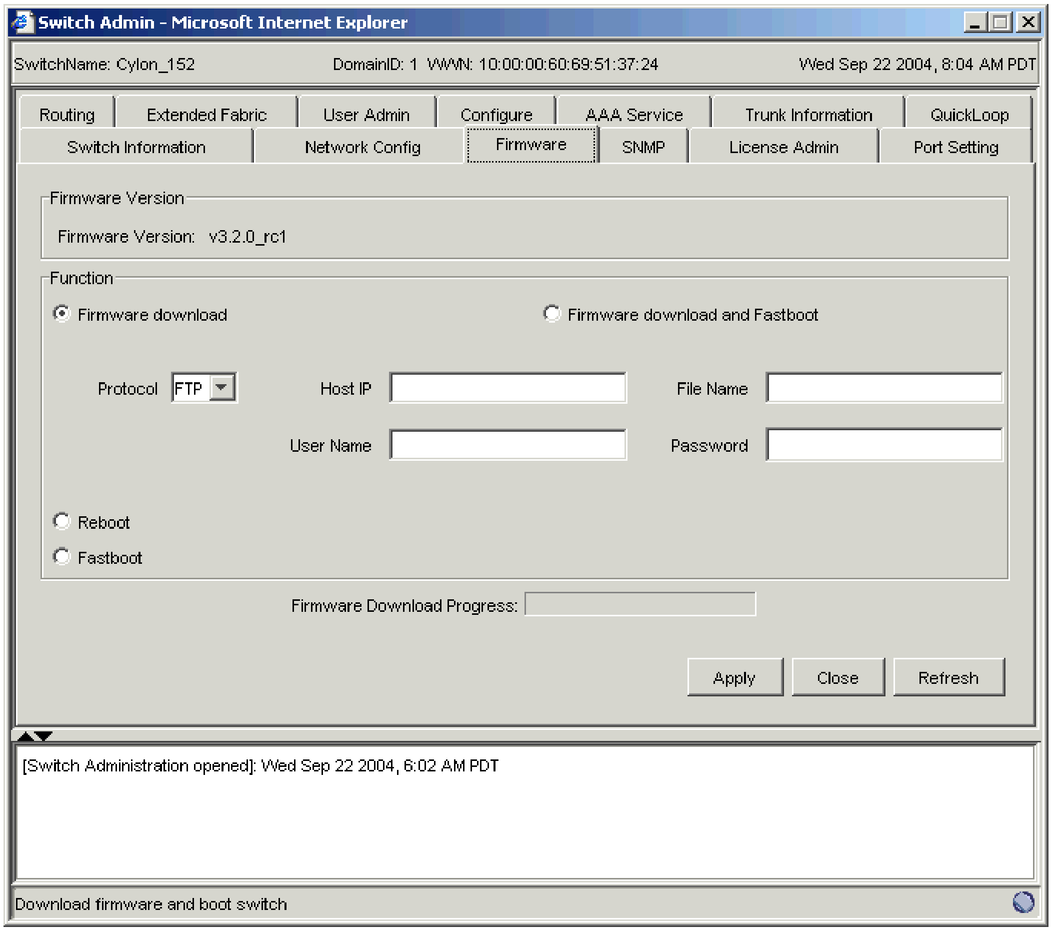
Use the **Firmware** tab to complete tasks such as:

- Downloading firmware
- Returning the switch to the original configuration
- Rebooting the switch

You must provide host information for the download firmware task.

Firmware Tab Example

An example of the **Firmware** tab is shown in Figure 8.



SwitchName: Cylon_152 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 8:04 AM PDT

Firmware Version: v3.2.0_rc1

● Firmware download ○ Firmware download and Fastboot

Protocol FTP Host IP File Name

User Name Password

○ Reboot

○ Fastboot

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Download firmware and boot switch

Figure 8: Firmware Tab

Firmware Field Descriptions

The Firmware fields are described in Table 3.

Table 3: Firmware field descriptions

Field	Description
Firmware Version	This field indicates the current firmware version running on the switch.
Firmware download	Select the radio button to download firmware.
Firmware download and Fastboot	Select the radio button to download firmware and then perform a fast boot of the switch.
Protocol	Select a download protocol: FTP or RSH. FTP requires a password to initiate file transfer; RSH does not. If you select RSH, the password field is removed.
Host IP	Enter the IP address of the host.
File Name	Enter the file name of the firmware package to be downloaded.
User Name	Enter the User Name for the owner of the firmware package on the host.
Password	Enter the password of the User who owns the firmware package on the host. This option is displayed only if you select the FTP protocol.
Fastboot	Select to perform a fast boot (no POST).
Reboot	Select to perform a Reboot. Post is an optional feature. Check the POST checkbox to enable Reboot with POST; uncheck this box to enable Reboot with no POST.
Firmware Download Progress	This is a progress bar indicating the firmware download progress.

On original page 106, replace the following heading:

Using the Upload/Download Tab

With this heading:

Using the Firmware Tab

On original page 106, under the heading “Performing a Firmware Download,” modify the following information.

Replace steps 3 and 4 with the following:

1. Select the **Firmware** tab.
2. Select the **Firmware download** radio button.

Add the following after step 8:

You can monitor the progress by looking at the Firmware Download Progress bar on the **Firmware** tab.

On original page 106, delete the sections “Backing Up a Firmware Config File” and “Performing a Config Download to Switch.”

On original page 106, after the section “Performing a Firmware Download,” add the following sections:

Performing a Fast Boot

To perform a fast boot of a switch:

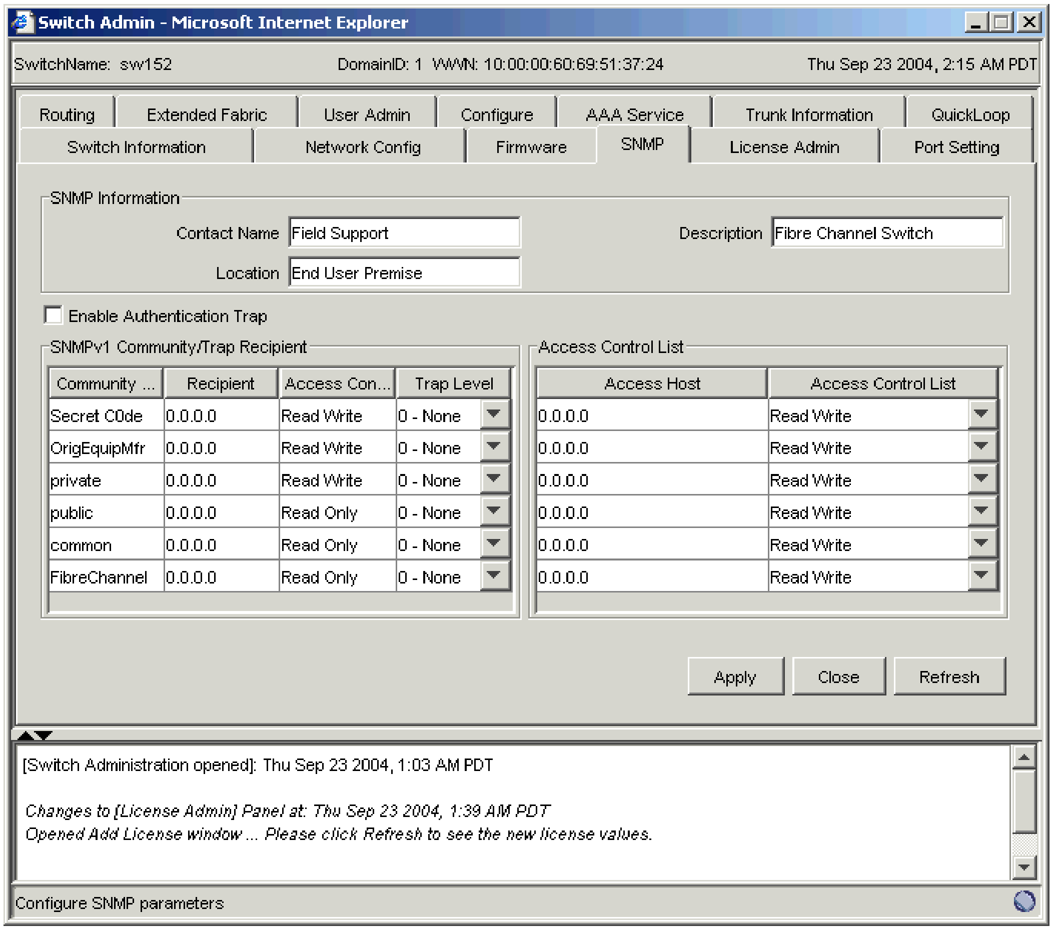
1. Access the Switch Admin Window (see “About the Switch Admin Window”).
2. Enter the admin user name and password.
3. Select the **Firmware** tab.
4. Click **Fastboot**.
5. Click **Apply**.

Performing a Reboot

To perform a reboot of a switch:

1. Access the Switch Admin Window (see “About the Switch Admin Window”).
2. Enter the admin user name and password.
3. Select the **Firmware** tab.
4. Click **Reboot**.
5. Click **Apply**.

On original page 109, under the heading “SNMP Tab Example,” replace original Figure 22, “SNMP Tab,” with the following:



SwitchName: sw152 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Thu Sep 23 2004, 2:15 AM PDT

SNMP Information

Contact Name: Field Support

Description: Fibre Channel Switch

Location: End User Premise

□ Enable Authentication Trap

SNMPv1 Community/Trap Recipient

Community ...	Recipient	Access Con...	Trap Level
Secret C0de	0.0.0.0	Read Write	0 - None
OrigEquipMfr	0.0.0.0	Read Write	0 - None
private	0.0.0.0	Read Write	0 - None
public	0.0.0.0	Read Only	0 - None
common	0.0.0.0	Read Only	0 - None
FibreChannel	0.0.0.0	Read Only	0 - None

Access Control List

Access Host	Access Control List
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write

[Switch Administration opened]: Thu Sep 23 2004, 1:03 AM PDT

Changes to [License Admin] Panel at: Thu Sep 23 2004, 1:39 AM PDT
Opened Add License window ... Please click Refresh to see the new license values.

Configure SNMP parameters

Figure 9: SNMP Tab (Secure Mode disabled)

On original page 110, in original Table 21, “SNMP Field Descriptions,” under the heading “SNMP Field Descriptions,” modify the following information.

Delete the following row:

Trap Level	Use to set the severity level of switch events that prompt SNMP traps. Default is 0.

Delete the following row:

Permissions	Displays the read/write access of a particular community string. READ ONLY access means that a member of a community string has the right to view, but cannot make changes. READ/WRITE access means that a member of a community string can be both viewed and make changes.

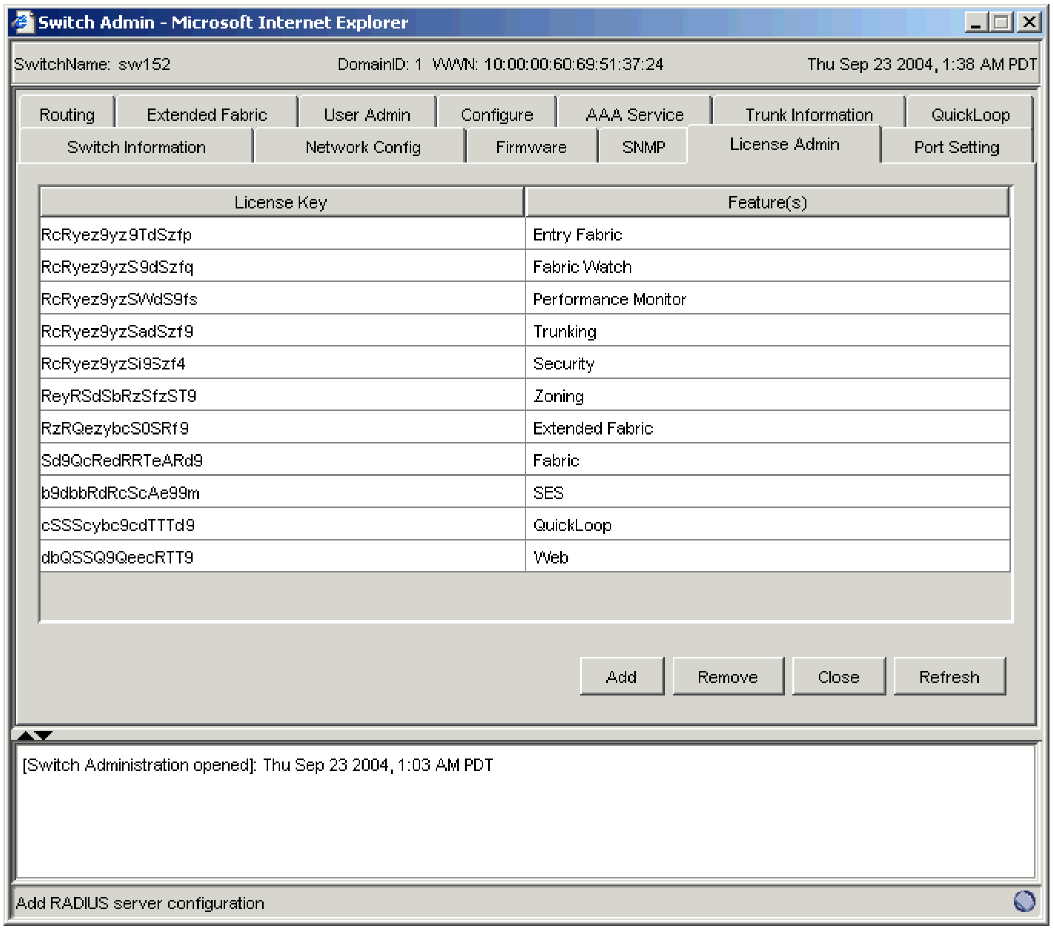
And replace it with these two rows:

Access Control	Displays the read/write access of a particular community string. READ ONLY access means that a member of a community string has the right to view, but cannot make changes. READ/WRITE access means that a member of a community string can be both viewed and make changes.
Trap Level	Use to set the severity level of switch events that prompt SNMP traps. Default is 0.

On original page 111, under the heading “Using the SNMP Tab to Set Trap Levels,” replace step 4 with the following:

6. For each recipient, select a Trap level from the pull-down menu. The level you select refers to the Event level that prompts a trap. See “About the Switch Events Button.”

On original page 112, under the heading “License Admin Tab Example,” replace original Figure 23, “License Admin Tab,” with the following:



SwitchName: sw152 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Thu Sep 23 2004, 1:38 AM PDT

License Key	Feature(s)
RcRyez9yz9TdSzfp	Entry Fabric
RcRyez9yzS9dSzfq	Fabric Watch
RcRyez9yzSWdS9fs	Performance Monitor
RcRyez9yzSadSzf9	Trunking
RcRyez9yzSi9Szf4	Security
ReyRSdSbRzSfzST9	Zoning
RzRQezybcS0SRf9	Extended Fabric
Sd9QcRedRRTeARd9	Fabric
b9dbbRdRcScAe99m	SES
cSSScybc9cdTTTd9	QuickLoop
dbQSSQ9QeecRTT9	Web

[Switch Administration opened]: Thu Sep 23 2004, 1:03 AM PDT

Add RADIUS server configuration

Figure 10: License Admin Tab

On original page 113, under the heading “License Admin Field Description,” delete the following row from original Table 22, “License Admin Field Descriptions”:

License Key field	Enter a license key to be added or double-click a license key from the LicenseKey column to have it display in this field.

On original page 114, under the heading "Add a License to a Switch," delete the following steps 4 and 5 from the procedure:

4. Enter a new license key in the License Key field.
5. Click the **Add** button.

And replace them with these three steps:

4. Click the **Add** button.
5. Type or paste the new license key in the License Key field.
6. Click the **Add License** button.

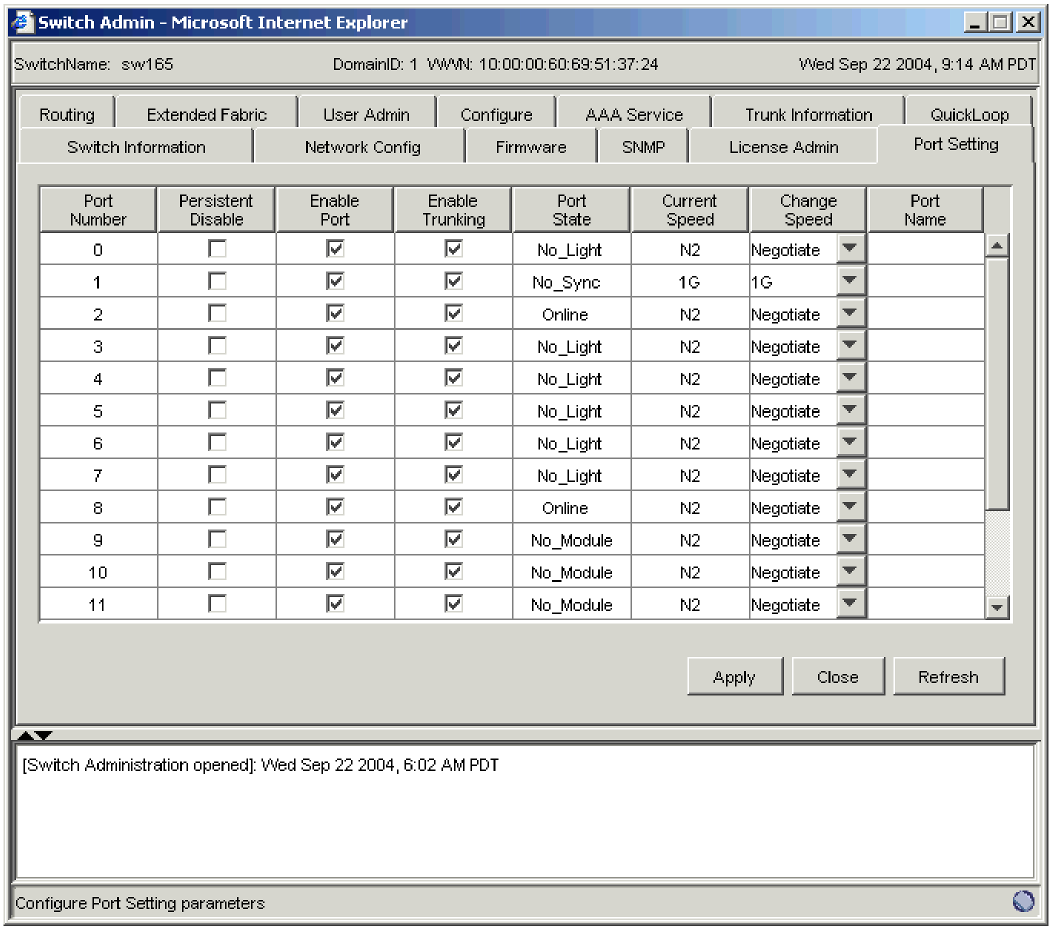
On original page 114, under the heading "Remove a License From a Switch," replace step 4:

4. Enter the license key to remove, or double-click a license key from the License Key column to display it in License Key field.

With this step:

4. Select a license key from the License Key column.

On original page 116, under the heading "Port Settings Tab Example," replace original Figure 24, "Port Setting Tab," with the following:



SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 9:14 AM PDT

Port Number	Persistent Disable	Enable Port	Enable Trunking	Port State	Current Speed	Change Speed	Port Name
0	□	☑	☑	No_Light	N2	Negotiate	
1	□	☑	☑	No_Sync	1G	1G	
2	□	☑	☑	Online	N2	Negotiate	
3	□	☑	☑	No_Light	N2	Negotiate	
4	□	☑	☑	No_Light	N2	Negotiate	
5	□	☑	☑	No_Light	N2	Negotiate	
6	□	☑	☑	No_Light	N2	Negotiate	
7	□	☑	☑	No_Light	N2	Negotiate	
8	□	☑	☑	Online	N2	Negotiate	
9	□	☑	☑	No_Module	N2	Negotiate	
10	□	☑	☑	No_Module	N2	Negotiate	
11	□	☑	☑	No_Module	N2	Negotiate	

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Configure Port Setting parameters

Figure 11: Port Setting Tab

On original page 118, under the heading "Enabling Trunking on a Port," replace step 4:

4. Check the Trunk box that corresponds to the port you wish to trunk.

With the following:

4. Check the Enabling Trunking box that corresponds to the port you want to trunk.

On original page 119, under the heading “Disabling a Port over Reboots,” replace step 4:

4. Select the slot and port you want to disable over reboots.

With the following:

4. Select the port you want to disable over reboots.

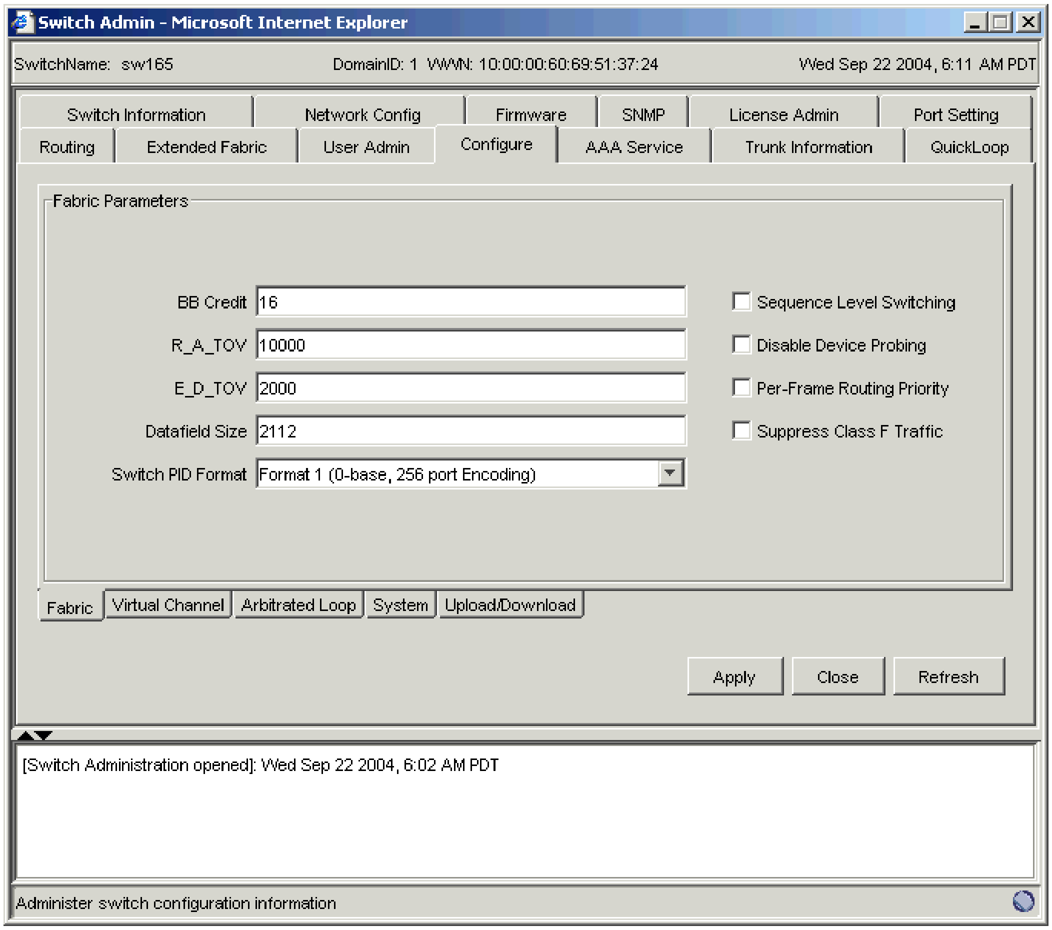
On original page 120, under the heading “About the Configure Tab,” replace the first sentence:

Use the Configure tab of the Administrative Interface to configure Fabric Parameters, Virtual Channel parameters, Arbitrated Loop parameters, and System Services parameters.

With this text:

Use the **Configure** tab of the Administrative Interface to configure Fabric Parameters, Virtual Channel parameters, Arbitrated Loop parameters, and System Services parameters, and to back up and download the switch configuration file.

On original page 121, under the heading “Configure (Fabric) Tab Example,” replace original Figure 25, “Configure (Fabric) Tab,” with the following:



SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 6:11 AM PDT

Fabric Parameters

BB Credit	16
R_A_TOV	10000
E_D_TOV	2000
Datafield Size	2112
Switch PID Format	Format 1 (0-base, 256 port Encoding)

□ Sequence Level Switching

□ Disable Device Probing

□ Per-Frame Routing Priority

□ Suppress Class F Traffic

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Administer switch configuration information

Figure 12: Configure (Fabric) Tab

On original page 122, in original Table 24, “Configure (Fabric) Field Descriptions,” modify the following information.

Replace the corresponding rows with the following:

Datafield Size	Use to configure (in bytes) the largest possible data field size. The valid range is 256 – 2112.
Sequence Level Switching	Select check box to enable frames of the same sequence from a particular group to be transmitted together. When this option is not selected, frames are transmitted interleaved among multiple sequences. Under normal circumstances, sequence-level switching should be disabled for better performance. However, some host adapters have issues when receiving interleaved frames among multiple sequences.

Suppress Class F Traffic	When checked, translative addressing (which allows private devices to communicate with public devices) is disabled.

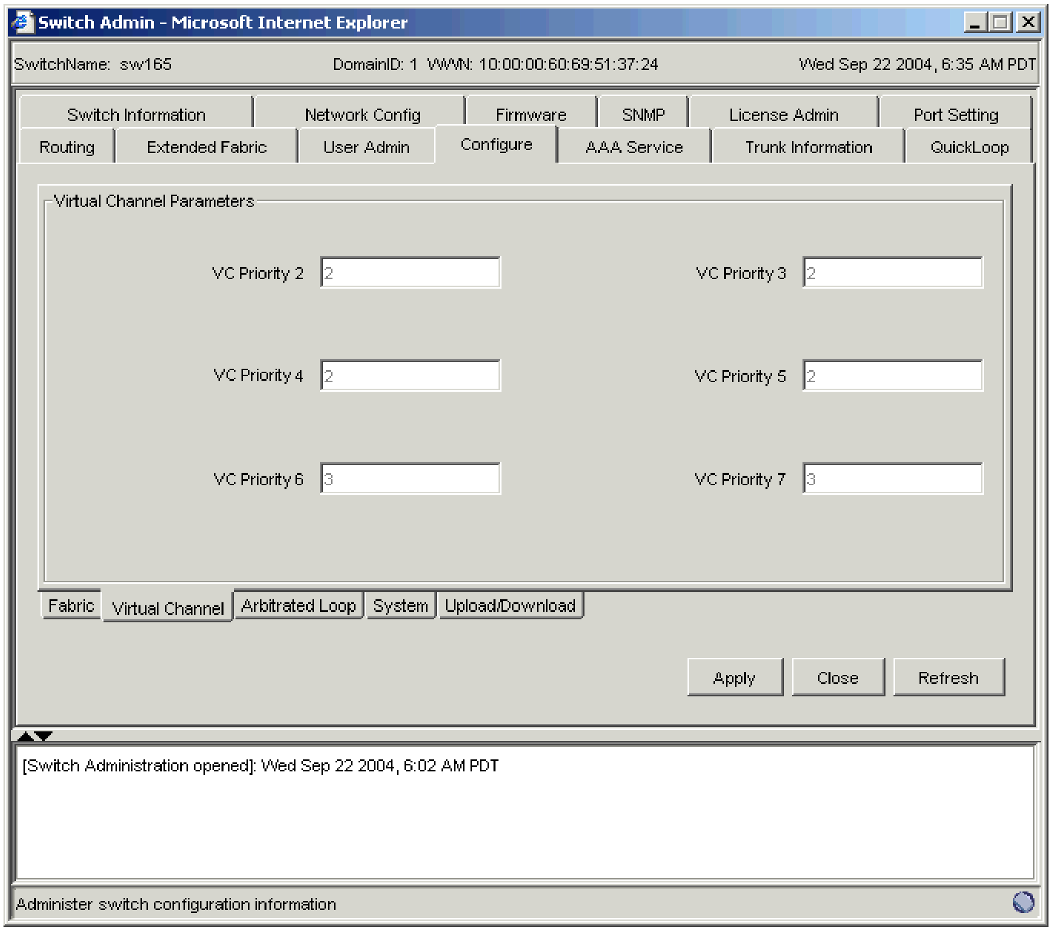
Add the following row:

Switch PID Format	Allows you to select a switch PID format from one of the following: ■ VC encoding – Set this format only if the fabric includes a Fibre Channel Storage Switch 8 or Fibre Channel Storage Switch 16. When set, the frame source and destination address use an address format that is compatible with Fibre Channel Storage Switch 8 and Fibre Channel Storage Switch 16. ■ Format 0 (16-port encoding) – Native format ■ Format 1 (0-base, 256-port encoding) – Core PID format ■ Format 2 (16-base, 256-port encoding) – Extended-edge PID format

Delete the following row:

VC Encoded Address Mode	Set this mode only if the fabric includes a Fibre Channel Storage Switch 8 or Fibre Channel Storage Switch 16. When set, the frame source and destination address use an address format that is compatible with Fibre Channel Storage Switch 8 and Fibre Channel Storage Switch 16. This option is grayed out if the switch is in interop mode.

On original page 124, under the heading “Configure (Virtual Channel) Tab Example,” replace original Figure 26, “Configure (Virtual Channel) Tab,” with the following:



SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 6:35 AM PDT

Virtual Channel Parameters

VC Priority 2: 2

VC Priority 3: 2

VC Priority 4: 2

VC Priority 5: 2

VC Priority 6: 3

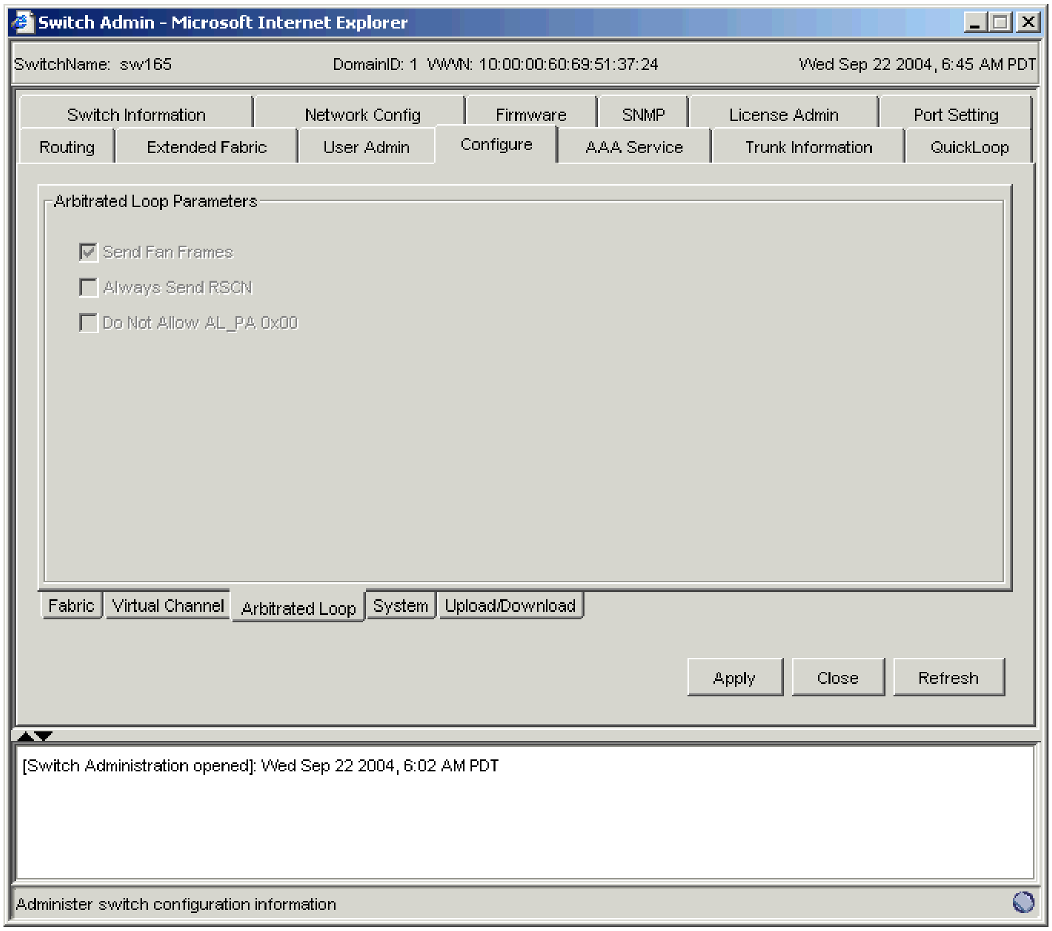
VC Priority 7: 3

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Administer switch configuration information

Figure 13: Configure (Virtual Channel) Tab

On original page 126, under the heading "Configure (Arbitrated Loop) Tab Example," replace original Figure 27, "Configure (Arbitrated Loop) Tab," with the following:



SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 6:45 AM PDT

Arbitrated Loop Parameters

☑ Send Fan Frames

□ Always Send RSCN

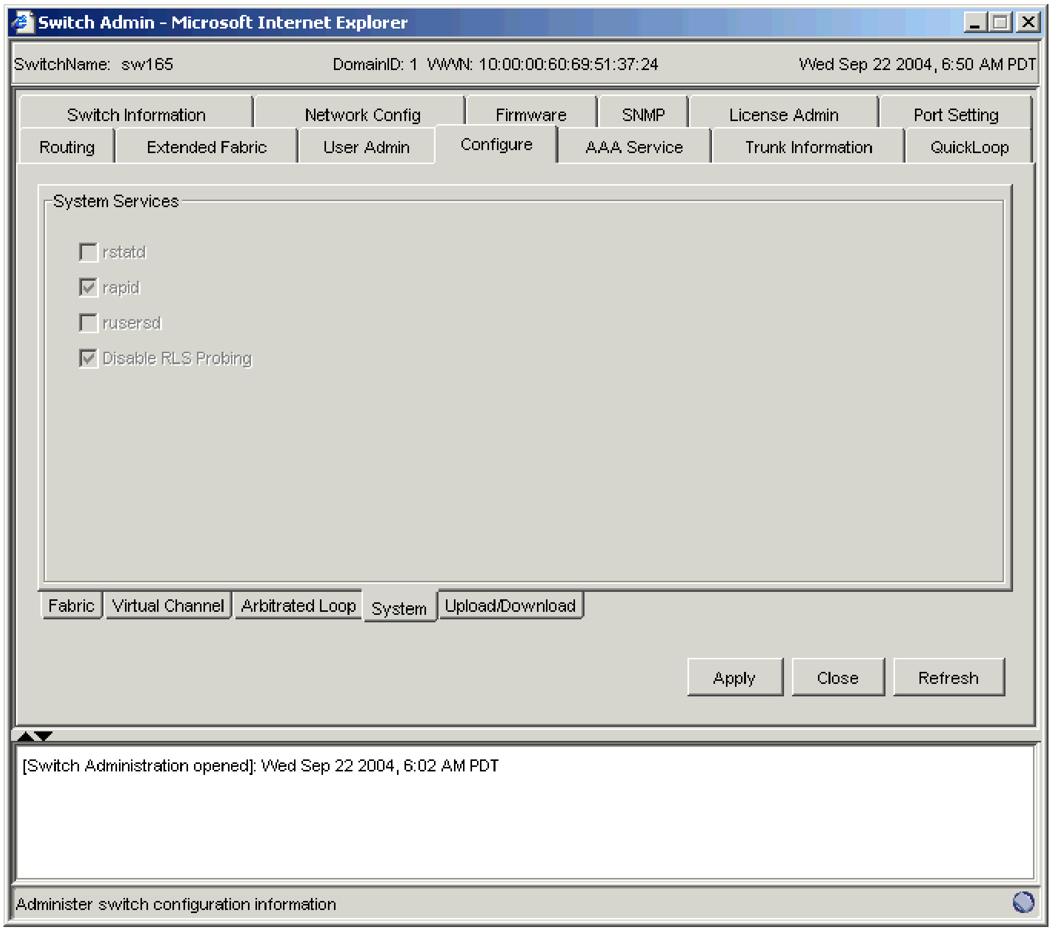
□ Do Not Allow AL_PA 0x00

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Administer switch configuration information

Figure 14: Configure (Arbitrated Loop) Tab

On original page 128, under the heading "Configure (System) Tab Example," replace original Figure 28, "Configure (System) Tab," with the following:



SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 6:50 AM PDT

System Services

□ rstatd
☑ rapid
□ rusersd
☑ Disable RLS Probing

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

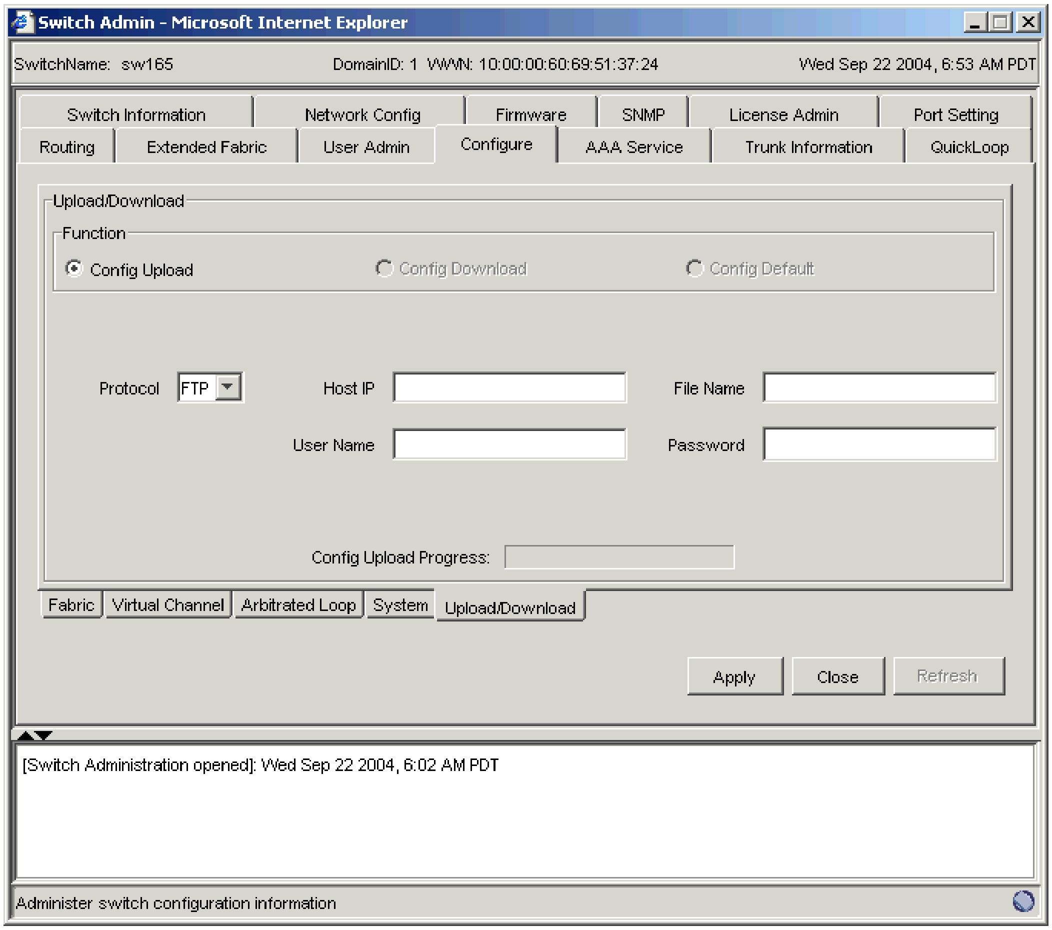
Administer switch configuration information

Figure 15: Configure (System) Tab

On original page 129, after the section "Configure (System) Field Descriptions," add the following sections:

Configure (Upload/Download) Tab Example

An example of the Configure (Upload/Download) Tab is shown in Figure 16.



SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 6:53 AM PDT

● Config Upload ○ Config Download ○ Config Default

Protocol FTP

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Administer switch configuration information

Figure 16: Configure (Upload/Download) Tab

Configure (Upload/Download) Field Descriptions

The fields available in the Configure (Upload/Download) Tab are described in Table 4.

Table 4: Configure (Upload/Download) Field Descriptions

Field	Description
Function radio buttons	Radio buttons indicating the function to be performed: Config Upload, Config Download, or Config Default.
Protocol	The protocol to use for the upload or download: either FTP or RSH.
Host IP	The host IP address.
File Name	The fully qualified path of the configuration file.
User Name	The user name for the host.
Password	The password for the host.
Config Upload Progress	A progress bar indicating the configuration upload or download progress.

On original page 130, after the heading "Using the Configure Tab to Configure FAN Frame Notification Parameters," add the following sections:

Backing Up a Switch Config File

To back up a firmware configuration file:

1. Access the Switch Admin Window (see "About the Switch Admin Window.")
2. Enter the admin user name and password.
3. Select the **Switch Information** tab.
4. Disable the switch.
5. Click the **Apply** button.
6. Select the **Configure** tab.
7. Select the **Upload/Download** subtab.
8. Select the **Config Upload to Host** radio button.
9. Enter the User Name, Password, and Host IP information.
10. Enter the name of the config file with a fully-qualified path.
11. Click **Apply**.

    You can monitor the progress by observing the Upload/Download Progress bar on the **Configure** tab.

Performing a Config Download to a Switch

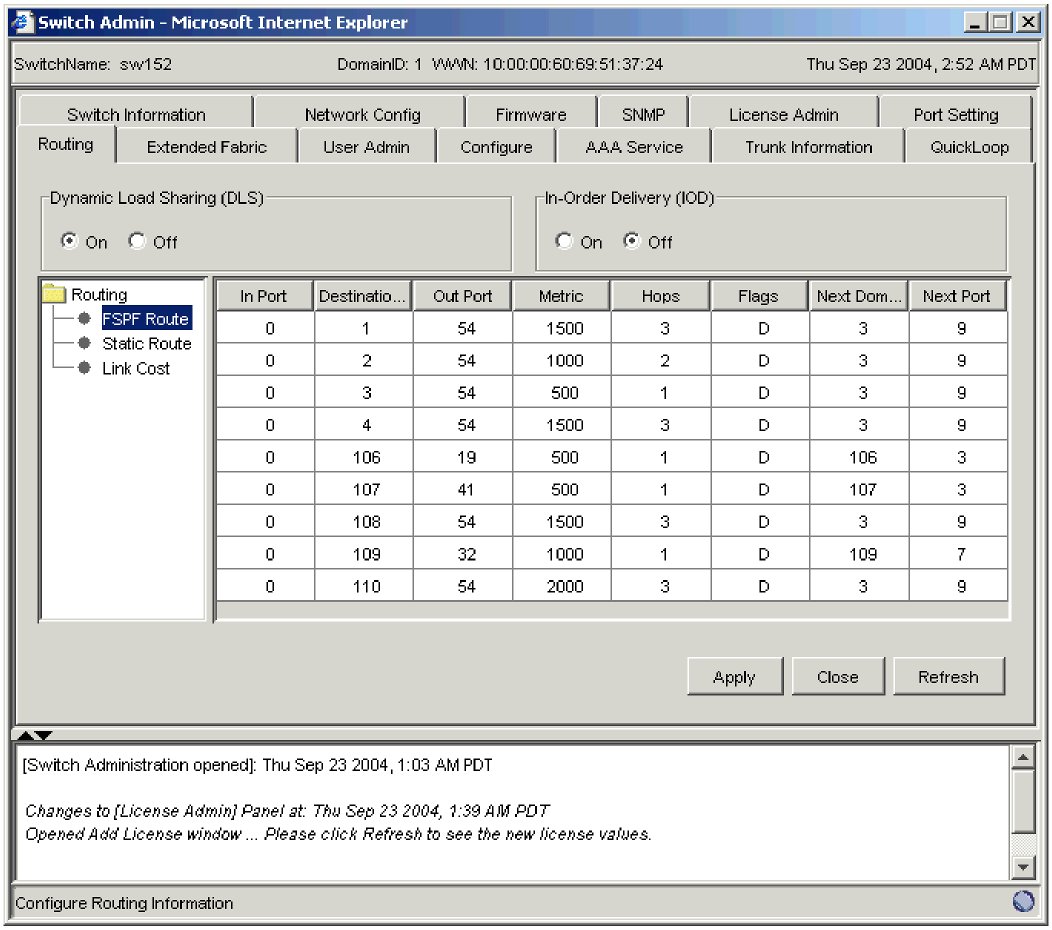
To download a configuration to the switch:

1. Access the Switch Admin Window (see "About the Switch Admin Window.")
2. Enter the admin user name and password.
3. Select the **Switch Information** tab.
4. Disable the switch.
5. Click the **Apply** button.
6. Select the **Configure** tab.

7. Select the **Upload/Download** subtab.
8. Select the **Config Download to Switch** radio button.
9. Enter the User Name, Password, and Host IP information.
10. Enter the name of the config file with a fully qualified path.
11. Click **Apply**.

    You can monitor the progress by looking at the Upload/Download Progress bar on the **Configure** tab.
12. Enable the switch.

On original page 132, under the heading "Routing (FSPF Route) Tab Example," replace original Figure 29, "Routing (FSPF Route) Tab," with the following:



SwitchName: sw152 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Thu Sep 23 2004, 2:52 AM PDT

Dynamic Load Sharing (DLS): ● On ○ Off

In-Order Delivery (IOD): ○ On ● Off

In Port	Destinatio...	Out Port	Metric	Hops	Flags	Next Dom...	Next Port
0	1	54	1500	3	D	3	9
0	2	54	1000	2	D	3	9
0	3	54	500	1	D	3	9
0	4	54	1500	3	D	3	9
0	106	19	500	1	D	106	3
0	107	41	500	1	D	107	3
0	108	54	1500	3	D	3	9
0	109	32	1000	1	D	109	7
0	110	54	2000	3	D	3	9

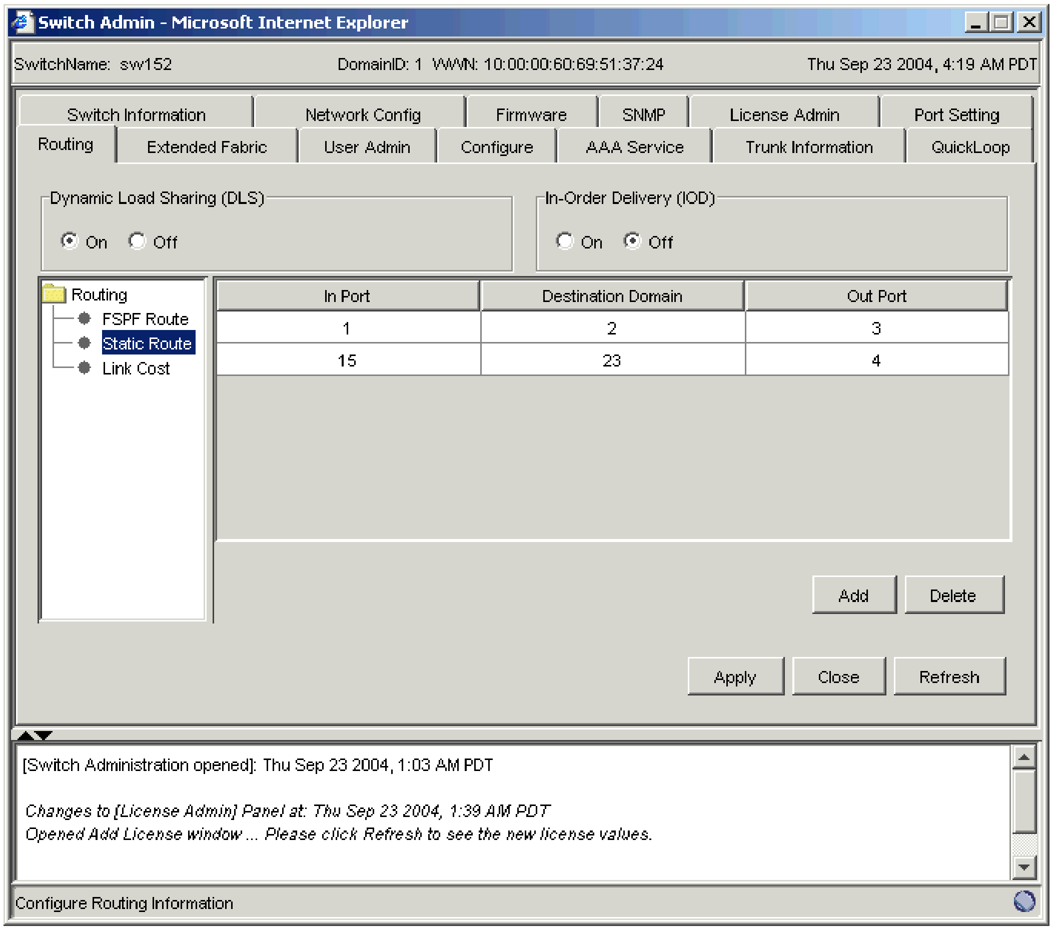
```
[Switch Administration opened]: Thu Sep 23 2004, 1:03 AM PDT

Changes to [License Admin] Panel at: Thu Sep 23 2004, 1:39 AM PDT
Opened Add License window ... Please click Refresh to see the new license values.
```

Configure Routing Information

Figure 17: Routing (FSPF Route) Tab

On original page 135, under the heading "Routing (Static Route) Tab Example," replace original Figure 30, "Routing (Static Route) Tab," with the following:



SwitchName: sw152 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Thu Sep 23 2004, 4:19 AM PDT

Dynamic Load Sharing (DLS): ● On ○ Off

In-Order Delivery (IOD): ○ On ● Off

In Port	Destination Domain	Out Port
1	2	3
15	23	4

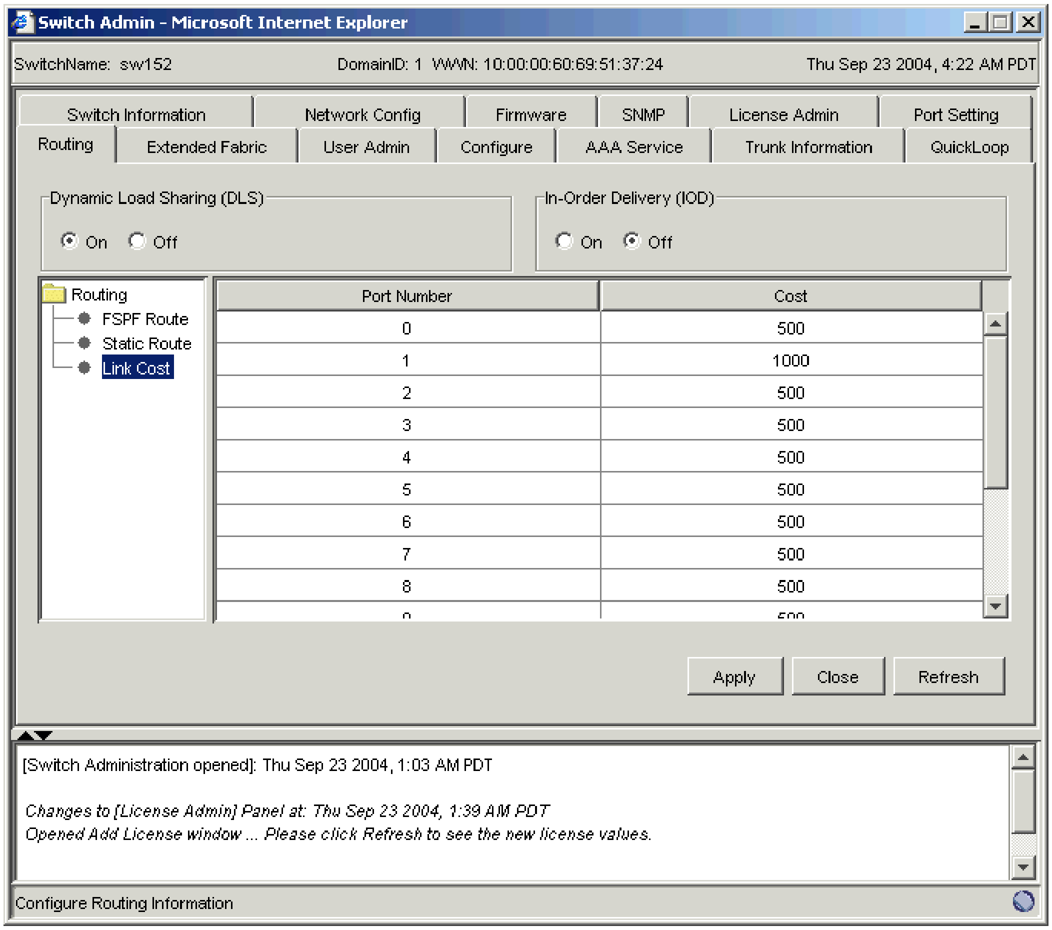
[Switch Administration opened]: Thu Sep 23 2004, 1:03 AM PDT

Changes to [License Admin] Panel at: Thu Sep 23 2004, 1:39 AM PDT
Opened Add License window ... Please click Refresh to see the new license values.

Configure Routing Information

Figure 18: Routing (Static Route) Tab

On original page 137, under the heading "Routing (Link Cost) Tab Example," replace original Figure 31, "Routing (Link Cost) Tab," with the following:



SwitchName: sw152 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Thu Sep 23 2004, 4:22 AM PDT

Dynamic Load Sharing (DLS) ● On ○ Off

In-Order Delivery (IOD) ○ On ● Off

Port Number	Cost
0	500
1	1000
2	500
3	500
4	500
5	500
6	500
7	500
8	500

[Switch Administration opened]: Thu Sep 23 2004, 1:03 AM PDT

Changes to [License Admin] Panel at: Thu Sep 23 2004, 1:39 AM PDT
Opened Add License window ... Please click Refresh to see the new license values.

Configure Routing Information

Figure 19: Routing (Link Cost) Tab

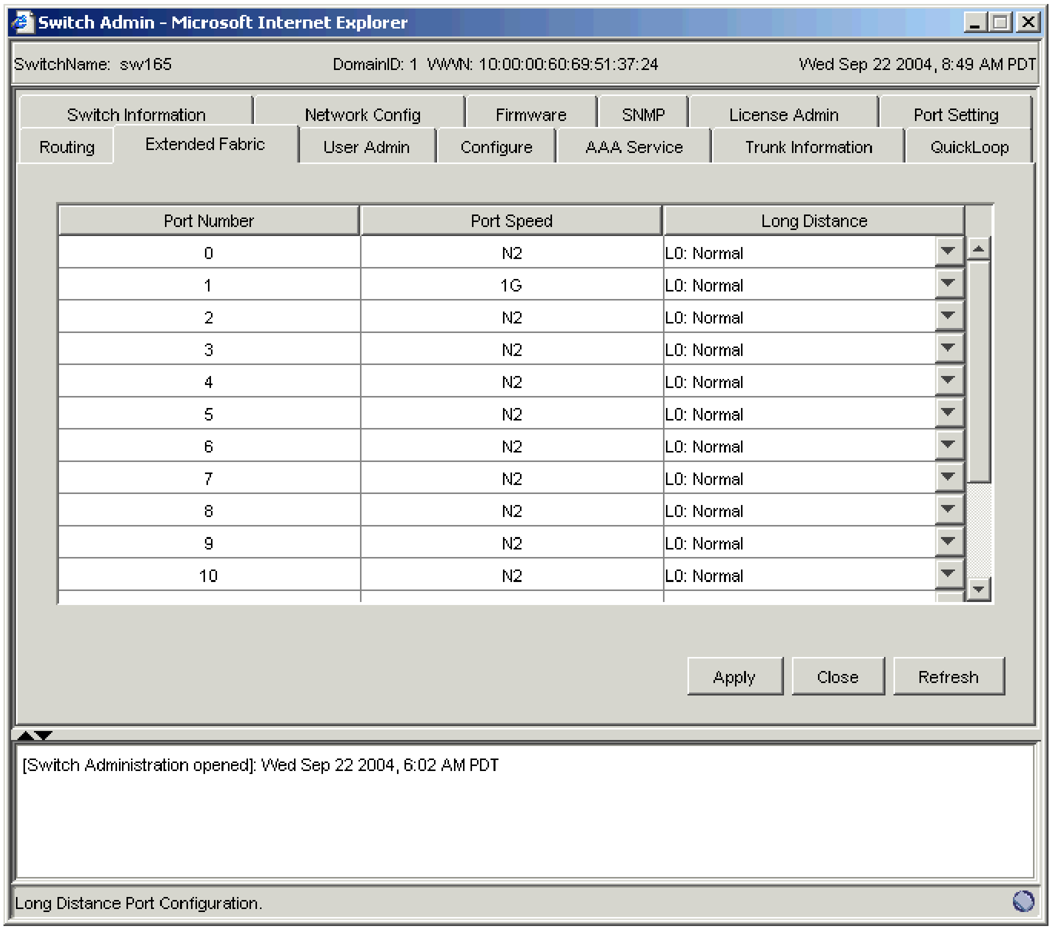
On original page 141 under the heading "Configuring Link Cost," add the following text to the end of step 6:

Setting the value to `0` sets the link cost to the default value for that port.

On original page 143, replace the section "Extended Fabrics Tab Example" with the following:

Extended Fabric Tab Example

An example of the **Extended Fabric** tab is shown in Figure 20.



SwitchName: sw165 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Wed Sep 22 2004, 8:49 AM PDT

Port Number	Port Speed	Long Distance
0	N2	L0: Normal
1	1G	L0: Normal
2	N2	L0: Normal
3	N2	L0: Normal
4	N2	L0: Normal
5	N2	L0: Normal
6	N2	L0: Normal
7	N2	L0: Normal
8	N2	L0: Normal
9	N2	L0: Normal
10	N2	L0: Normal

[Switch Administration opened]: Wed Sep 22 2004, 6:02 AM PDT

Long Distance Port Configuration.

Figure 20: Extended Fabric Tab

On original pages 143 and 144, under the heading "Extended Fabric Field Descriptions," modify the following.

Replace the first sentence with:

The fields available in the **Extended Fabric** tab are described in Table 33.

In original Table 33, "Extended Fabric Field Descriptions," delete the following rows:

Extended Fabric Mode	
Enable	Click the radio button to enable the Extended Fabric mode. The switch must be disabled to enable the Extended Fabric mode.
Disable	Click to disable the Extended Fabric Mode.

VCXLT Link Init Enabled	Check the box to enable Virtual Channel link translation. See "About the Upload/Download Tab."

Replace the following row:

Port Speed	Displays the current port speed. The possible port speeds are described in "About the Upload/Download Tab."

With this row:

Port Speed	Displays the current port speed. The possible port speeds are described in "About the Upload/Download Tab."

On original page 145, under the heading "Using the Extended Fabric Tab to Configure a Port For Long-Distance," delete steps 4 and 5:

4. Click the **Enable** radio button.
5. Check the VCXLT box.

In step 6, delete the following text:

For information about the various distances, see "About the Upload/Download Tab."

On original page 145, after the section "Using the Extended Fabric Tab to Configure a Port For Long-Distance," add the following sections:

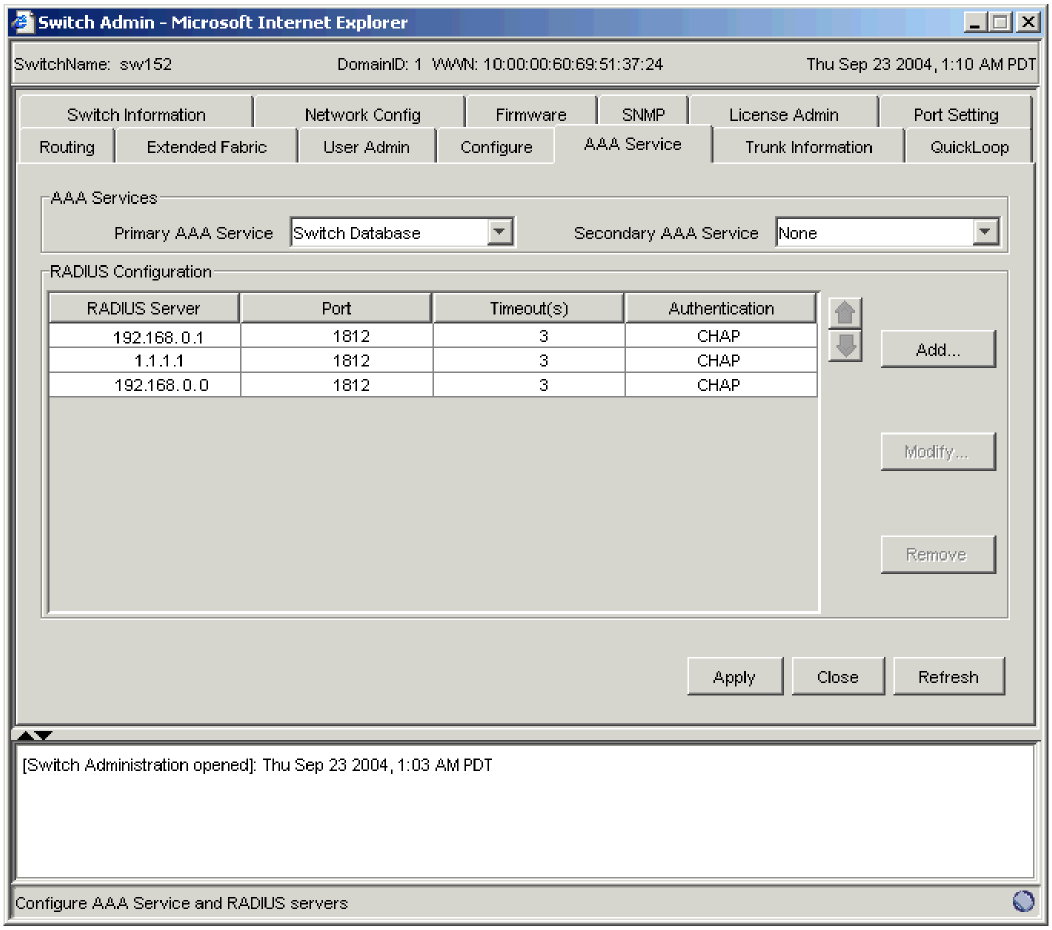
About the AAA Service Tab

Use the **AAA Service** tab to manage the RADIUS server. Through the **AAA Service** tab, you can perform the following tasks:

- Enable and disable the RADIUS server
- Configure the RADIUS server
- Modify the RADIUS server
- Modify the order of the RADIUS servers
- Remove a RADIUS server

AAA Service Tab Example

An example of the **AAA Service** tab is shown in Figure 21.



SwitchName: sw152 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Thu Sep 23 2004, 1:10 AM PDT

Primary AAA Service: Switch Database

Secondary AAA Service: None

RADIUS Server	Port	Timeout(s)	Authentication
192.168.0.1	1812	3	CHAP
1.1.1.1	1812	3	CHAP
192.168.0.0	1812	3	CHAP

[Switch Administration opened]: Thu Sep 23 2004, 1:03 AM PDT

Configure AAA Service and RADIUS servers

Figure 21: AAA Service Tab

AAA Service Tab Field Descriptions

Descriptions of the fields available in the **AAA Service** tab are shown in Table 5.

Table 5: AAA Service Tab Field Descriptions

Field	Description
AAA Services	
Primary AAA Service	Displays the name of the primary AAA service.
Secondary AAA Service	Displays the name of the secondary AAA service.
RADIUS Configuration	
RADIUS Server	Displays the name of the RADIUS server, which is either an IP address or a Dynamic Name String (DNS).
Port	Displays the port number.
Timeouts	Displays the timeout time, in minutes.
Authentication	Displays the authentication protocol: either CHAP or PAP.

Using the AAA Service Tab

Enabling and Disabling the RADIUS Server

You must be logged in as admin to configure the RADIUS server.

To configure the RADIUS server:

1. Access the Switch Admin Window (see “About the Switch Admin Module.”)
2. Enter the admin user name and password.
3. Select the **AAA Service** tab.
4. To enable RADIUS Service, select a RADIUS Service as the primary authentication, authorization, and acounting (AAA) service. You can set the secondary AAA service as None or Switch Database.

   To disable RADIUS Service, select Switch Database as the primary AAA service and None as the secondary service.
5. Click the **Apply** button.

Configuring the RADIUS Server

You can configure the RADIUS server even if it is disabled; you can configure up to five RADIUS servers. You must be logged in as admin to configure the RADIUS server.

To configure the RADIUS server:

1. Access the Switch Admin Window (see “About the Switch Admin Module.”)
2. Enter the admin user name and password.
3. Select the **AAA Service** tab.
4. Click **Add**. You can configure up to five RADIUS servers. If five RADIUS servers are already configured, the **Add** button is disabled.

The RADIUS Configuration dialog box opens.

5. Enter the RADIUS server name, which should be a valid IP address or DNS. Each RADIUS server should have a unique IP address or DNS name for the RADIUS server.
6. Optional: Enter the port number.
7. Optional: Enter the secret string.
8. Optional: Enter the timeout time in minutes.
9. Optional: Select an authentication protocol from CHAP or PAP. The default value is CHAP and, if you do not change it, CHAP will be the authentication protocol.
10. Click **OK**.
11. Click the **Apply** button.

Modifying the RADIUS Server

To modify the RADIUS server:

1. Access the Switch Admin Window (see “About the Switch Admin Module.”)
2. Enter the admin user name and password.
3. Select the **AAA Service** tab.
4. Select a RADIUS server from the RADIUS Configuration list.
5. Click **Modify**.

   The RADIUS Configuration dialog box opens.
6. Edit the RADIUS server name, which should be a valid IP address or Dynamic Name String (DNS). Each RADIUS server should have a unique IP address or DNS name for the RADIUS server.
7. Optional: Edit the port number.
8. Optional: Edit the secret string.
9. Optional: Edit the timeout time in minutes.
10. Optional: Select an authentication protocol from CHAP or PAP. The default value is CHAP; if you do not change it, CHAP will be the authentication protocol.
11. Click **OK**.
12. Click the **Apply** button.

Modifying the RADIUS Server Order

The RADIUS servers are contacted in the order they are listed, starting from the top of the list.

To modify the order that the RADIUS servers are contacted:

1. Access the Switch Admin Window (see “About the Switch Admin Module.”)
2. Enter the admin user name and password.
3. Select the **AAA Service** tab.
4. Select a RADIUS server from the RADIUS Configuration list.
5. Click the up and down arrows to rearrange the order of the RADIUS servers.
6. Click **OK**.
7. Click the **Apply** button.

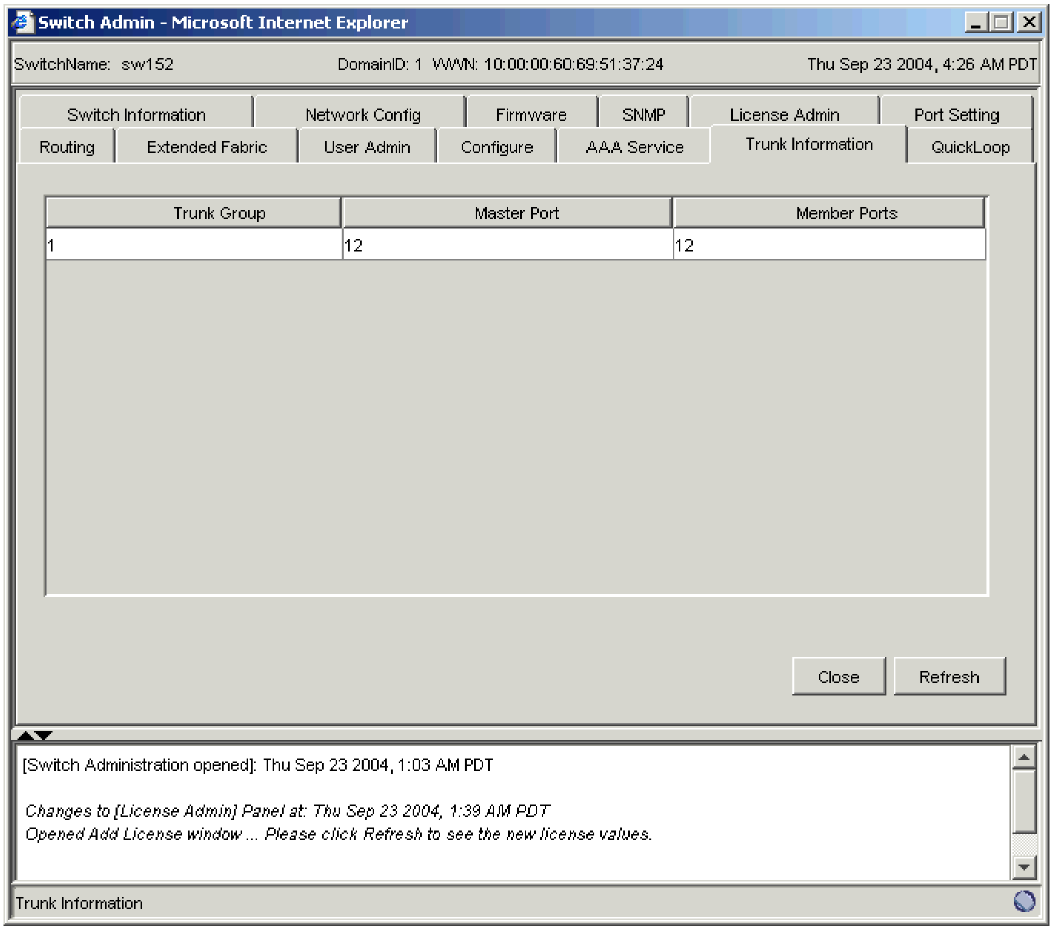
Removing a RADIUS Server

To remove a RADIUS server:

1. Access the Switch Admin Window (see “About the Switch Admin Module.”)
2. Enter the admin user name and password.
3. Select the **AAA Service** tab.
4. Select a RADIUS server from the RADIUS Configuration list.
5. Click **Remove**. If there is no RADIUS server configured, the Remove button is disabled. You cannot remove the only RADIUS server if the RADIUS service is the primary AAA service.

   The RADIUS server is not deleted until you apply the changes from the AAA Services tab.
6. Click the **Apply** button.

On original page 146, under the heading “Trunk Information Tab Example,” replace original Figure 33, “Trunk Information Tab,” with the following:



SwitchName: sw152 DomainID: 1 WWN: 10:00:00:60:69:51:37:24 Thu Sep 23 2004, 4:26 AM PDT

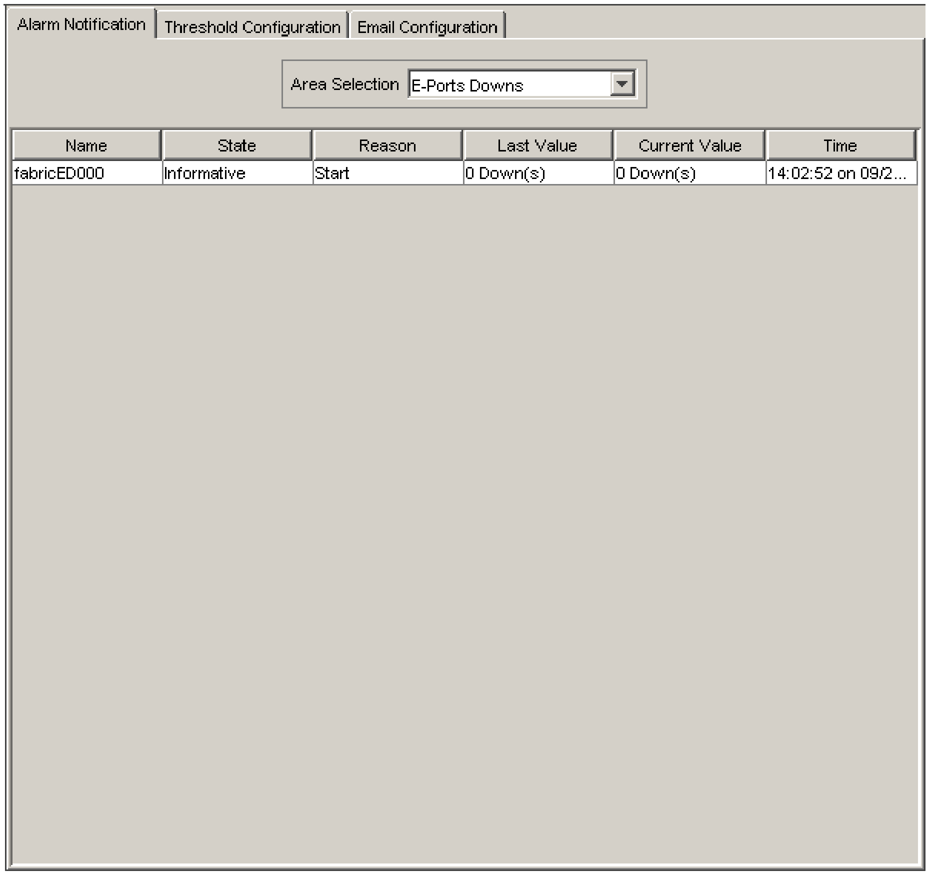
Trunk Group	Master Port	Member Ports
1	12	12

```
[Switch Administration opened]: Thu Sep 23 2004, 1:03 AM PDT

Changes to [License Admin] Panel at: Thu Sep 23 2004, 1:39 AM PDT
Opened Add License window ... Please click Refresh to see the new license values.
```

Figure 22: Trunk Information Tab

On original page 174, replace original Figure 41, “Alarm Notification Tab of Fabric Watch,” with the following:



Area Selection: E-Ports Downs

Name	State	Reason	Last Value	Current Value	Time
fabricED000	Informative	Start	0 Down(s)	0 Down(s)	14:02:52 on 09/2...

Figure 23: Alarm Notification Tab

On original page 175, in original Table 41, “Alarm Notification Field Descriptions,” replace the following row:

Selected Area	Displays the configurable areas in the drop-down menu. The items listed will change depending on the item selected in the Navigation tree.

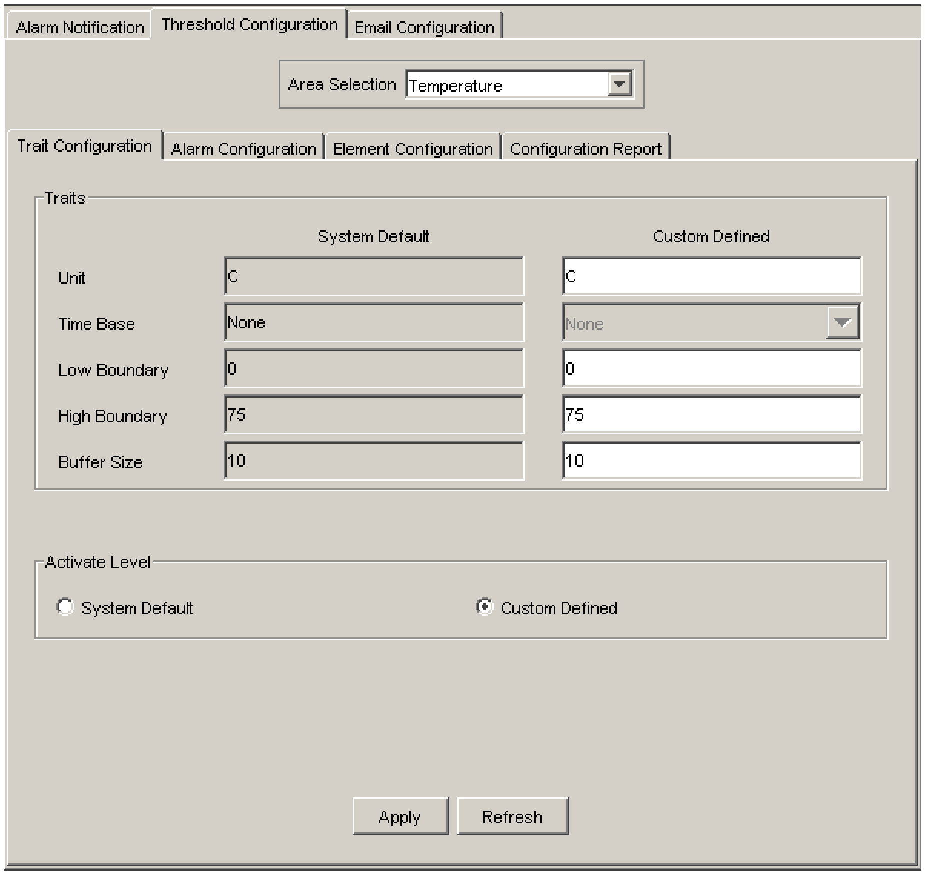
With this row:

Area Selection	Displays the configurable areas in the drop-down menu. The items listed change, depending on the item selected in the Navigation tree.

On original page 177, delete the section "About the Threshold Configuration Tab."

On original page 177, in the section "Threshold Configuration Tab Example," replace the text and the original Figure 42, "Threshold Configuration Area Configuration Tab," with the following:

The **Threshold Configuration Tab** > **Trait Configuration Tab** is shown in Figure 24.



Area Selection: Temperature

Traits

	System Default	Custom Defined
Unit	C	C
Time Base	None	None
Low Boundary	0	0
High Boundary	75	75
Buffer Size	10	10

Activate Level

○ System Default ● Custom Defined

Figure 24: Threshold Configuration Area Configuration Tab

On original pages 177 and 178, add the following table after original Figure 42, "Threshold Configuration Area Configuration Tab":

Table 6: Threshold Configuration Tab Components

Component	Description
Area Selection pull-down menu	Lists the areas of thresholds that you can configure. The areas that appear in the pull-down menu depend on the class that you select from the Fabric Watch Navigation tree.
Trait Configuration tab	Provides fields to configure Fabric Watch threshold boundaries and alarms. For more information, see "Trait Configuration Tab."
Alarm Configuration tab	Provides fields to configure Fabric Watch alarms. For more information, see "Alarm Configuration Tab."
Element Configuration tab	Provides fields to configure Fabric Watch threshold traits. For more information, see "Element Configuration Tab."
Configuration Report tab	Displays the Fabric Watch settings for the class that you select from the Fabric Watch navigation tree. For more information, see "Configuration Report Tab."

On original page 178, before the section "Threshold Notification Fields Descriptions," insert the following sections:

Trait Configuration Tab

Table 7 describes the components of the **Trait Configuration** tab.

Table 7: Trait Configuration Components

Component	Description
Unit field	Sets or displays the selected unit values used for the chosen area. Depending on the area of interest, this is figured in units of downs, reconfigs, errors, changes, logins, and so on.
Time Base pull-down menu	Sets or displays the basic unit of time in which events are recorded for the selected area. The units available from the pull-down menu are none, second, minute, hour, or day.
Low Boundary field	Sets or displays the number of low boundaries (the lowest limit at which an element does not trigger an event) for the selected area.
High Boundary field	Sets or displays the number of high boundaries (the highest limit at which an element does not trigger an event) for the selected area.
Buffer Size field	Sets or displays the threshold boundary buffer size of the selected area.
Activate Level radio buttons	Selects either System Default or Custom Defined to indicate which traits are to be activated.

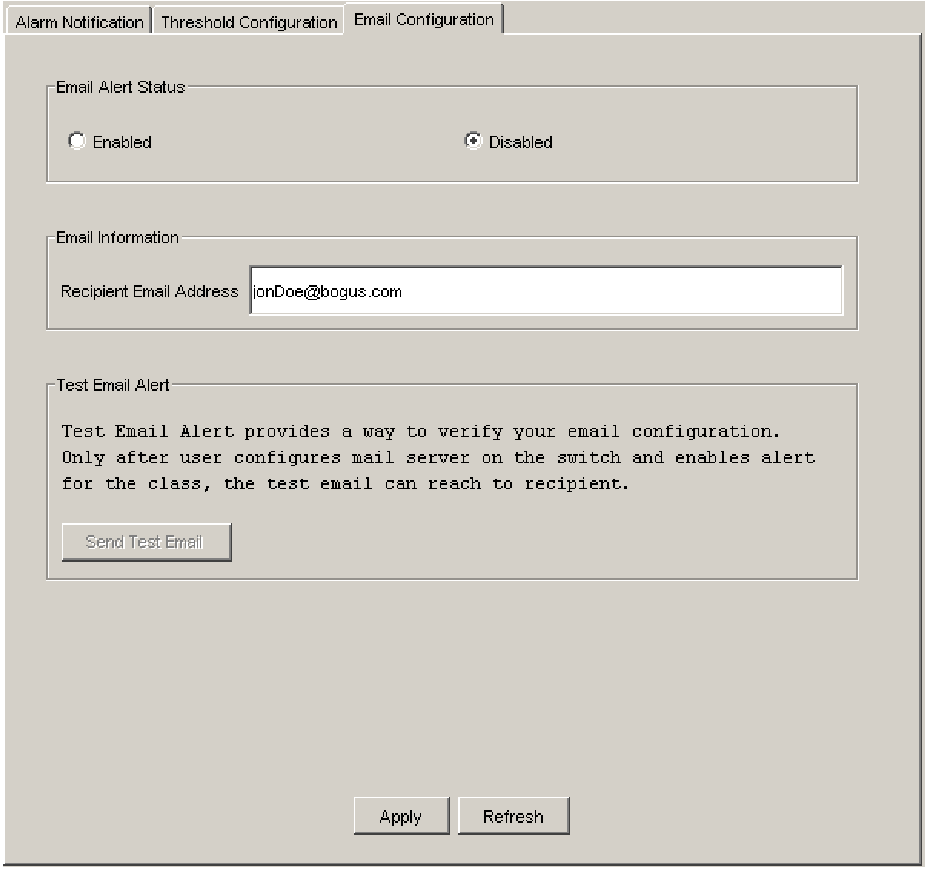
Alarm Configuration Tab

Table 8 lists and describes the components of the **Alarm Configuration** tab.

Table 8: Alarm Configuration Components

Component	Description
System Default and Custom Defined checkboxes	Select Alarm settings for Errorlog, SNMP, RAN, Portlog, and Email to be active on the switch side.
Activate Level radio buttons	Select either System Default or Custom Defined to indicate which traits are to be activated.

On original page 183, replace original Figure 43, “Email Configuration Tab,” with the following:



Recipient Email Address: jonDoe@bogus.com

Test Email Alert provides a way to verify your email configuration. Only after user configures mail server on the switch and enables alert for the class, the test email can reach to recipient.

Figure 25: Email Configuration Tab

On original page 181, under the heading "Configuring Boundary and Alarm Settings," replace the procedure in the section with the following:

To configure threshold boundaries and alarms, perform the following steps:

1. Access Fabric Watch (see "Access Fabric Watch.")
2. In the Fabric Watch Navigation tree, click the class that you want configure.
3. Select the **Threshold Configuration** tab.
4. Select the **Trait Configuration** subtab.
5. From the Select Area pull-down menu, select the area that you want to configure.

   The System Default traits are displayed for the selected class and area. If you do not want to change the system default settings, you do not need to finish the steps in this procedure.

   If you want to change the system default settings, proceed to the next step.
6. Enter custom values in the trait fields (such as Unit, High Boundary, and Low Boundary) in the Traits partition.
7. Select the **Custom Defined** radio button.
8. Click **Apply**.
9. Select the **Alarm Configuration** tab.

   The System Default alarms are displayed for the selected class and area. If you do not want to change the system default settings, you do not need to finish the steps in this procedure.

   If you want to change the system default settings, proceed to the next step.
10. Click a check box to set an alarm for an event type (Changed, exceeded, below, above, or in between) and the corresponding alarm action (ERROR_LOG, SNMP_TRAP, RAPI_TRAP, or EMAIL_ALERT).
11. Click **Custom Defined** in the Activate Level area.
12. Click **Apply**.

On original page 182, under the heading "View an Alarm Configuration Report," modify the following information.

In the procedure, replace step 5:

5. Select the alarm area report to be viewed from the Area drop-down menu.

With this text:

5. Select the alarm area report to be viewed from the Area Selection drop-down menu.

Delete step 6.

On original page 184, replace original Table 45, "Email Configuration Field Descriptions," with the following:

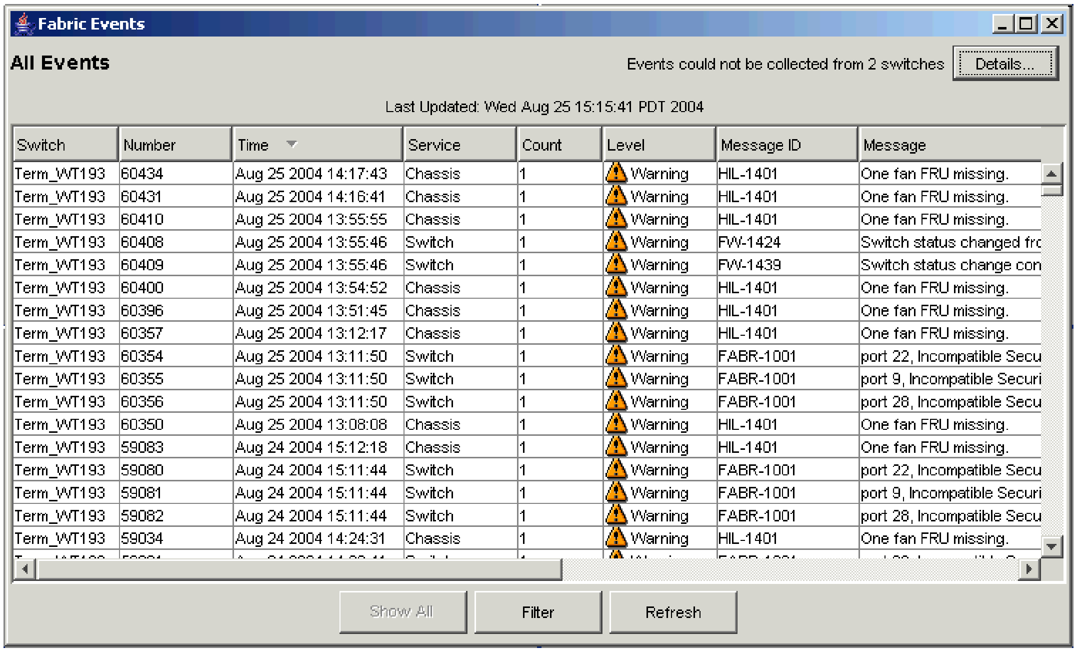
Table 9: Email Configuration Field Descriptions

Field	Description
Email Alert Status	
Enabled/Disabled	Select the Enabled or Disabled radio button to enable or disable email alarm notifications.
Email Information	
Recipient Email Address	Enter a valid mail recipient email address.
Test Email Alert	
Send Test Email	Select this button to send a validation email.

On original page 190, in the section "About Fabric Events," replace the text with the following:

The Fabric Events window provides a running log of events for all switches in the fabric. Events are displayed for all switches in the fabric in the Fabric Events window. Fabric events can be collected only for switches that have the same security level as the launch switch. Fabric events are not automatically polled. You must click **Refresh** from the Fabric Events window to poll fabric events. For switches that have a different level of security from the launch switch, a number is displayed, indicating how many switches have no events reported from the last polling. For detailed information on the switch names and reasons for not polling (if available), click **Details**.

On original page 190, under the heading "Fabric Events Example," replace original Figure 45, "The Fabric Events Window," with the following:



All Events

Events could not be collected from 2 switches

Last Updated: Wed Aug 25 15:15:41 PDT 2004

Switch	Number	Time	Service	Count	Level	Message ID	Message
Term_WT193	60434	Aug 25 2004 14:17:43	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60431	Aug 25 2004 14:16:41	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60410	Aug 25 2004 13:55:55	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60408	Aug 25 2004 13:55:46	Switch	1	⚠ Warning	FW-1424	Switch status changed frc
Term_WT193	60409	Aug 25 2004 13:55:46	Switch	1	⚠ Warning	FW-1439	Switch status change con
Term_WT193	60400	Aug 25 2004 13:54:52	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60396	Aug 25 2004 13:51:45	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60357	Aug 25 2004 13:12:17	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60354	Aug 25 2004 13:11:50	Switch	1	⚠ Warning	FABR-1001	port 22, Incompatible Secu
Term_WT193	60355	Aug 25 2004 13:11:50	Switch	1	⚠ Warning	FABR-1001	port 9, Incompatible Securi
Term_WT193	60356	Aug 25 2004 13:11:50	Switch	1	⚠ Warning	FABR-1001	port 28, Incompatible Secu
Term_WT193	60350	Aug 25 2004 13:08:08	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	59083	Aug 24 2004 15:12:18	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	59080	Aug 24 2004 15:11:44	Switch	1	⚠ Warning	FABR-1001	port 22, Incompatible Secu
Term_WT193	59081	Aug 24 2004 15:11:44	Switch	1	⚠ Warning	FABR-1001	port 9, Incompatible Securi
Term_WT193	59082	Aug 24 2004 15:11:44	Switch	1	⚠ Warning	FABR-1001	port 28, Incompatible Secu
Term_WT193	59034	Aug 24 2004 14:24:31	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.

Figure 26: The Fabric Events Window

On original page 191, after the section "Accessing Fabric Events," add the following sections:

Filtering Fabric Events

You can filter the events in the Fabric Events window by time and severity. You can apply just one type of filter at a time or all types of filters at the same time. Click the **Filter** button to display the Event Filter dialog box.

When a filter is applied, the **Show All** button is active in the Events Report and the types of filters applied are identified at the top of the Events Report. To un-apply a filter, click the **Show All** button in the Events Report.

Filtering Events by Time Intervals

To filter events by time intervals:

1. Access Web Tools.
2. Find the Fabric tool bar.
3. Select the **Fabric Events** icon in the lower corner of the Fabric Tree.

   The Fabric Events window opens.
4. Click **Filter**.

   The Event Filter dialog box opens.

5. Optional: To filter events within a certain time period:
   a. Click **From** and enter the start time and date in the fields.
   b. Click **To** and enter the finish time and date in the fields.
6. Optional: To filter all events beginning at a certain date and time, click **From** and enter the start time and date in the fields.
7. Optional: To filter events up until a certain date and time, click **To** and enter the finish time and date in the fields.
8. Click **OK**.

   The filter is enabled and the enabled filter type is displayed in the Events Report.

Filtering Events by Event Severity

To filter events by event severity levels:

1. Access Web Tools.
2. Find the Fabric tool bar.
3. Select the Fabric Events icon in the lower corner of the Fabric Tree.

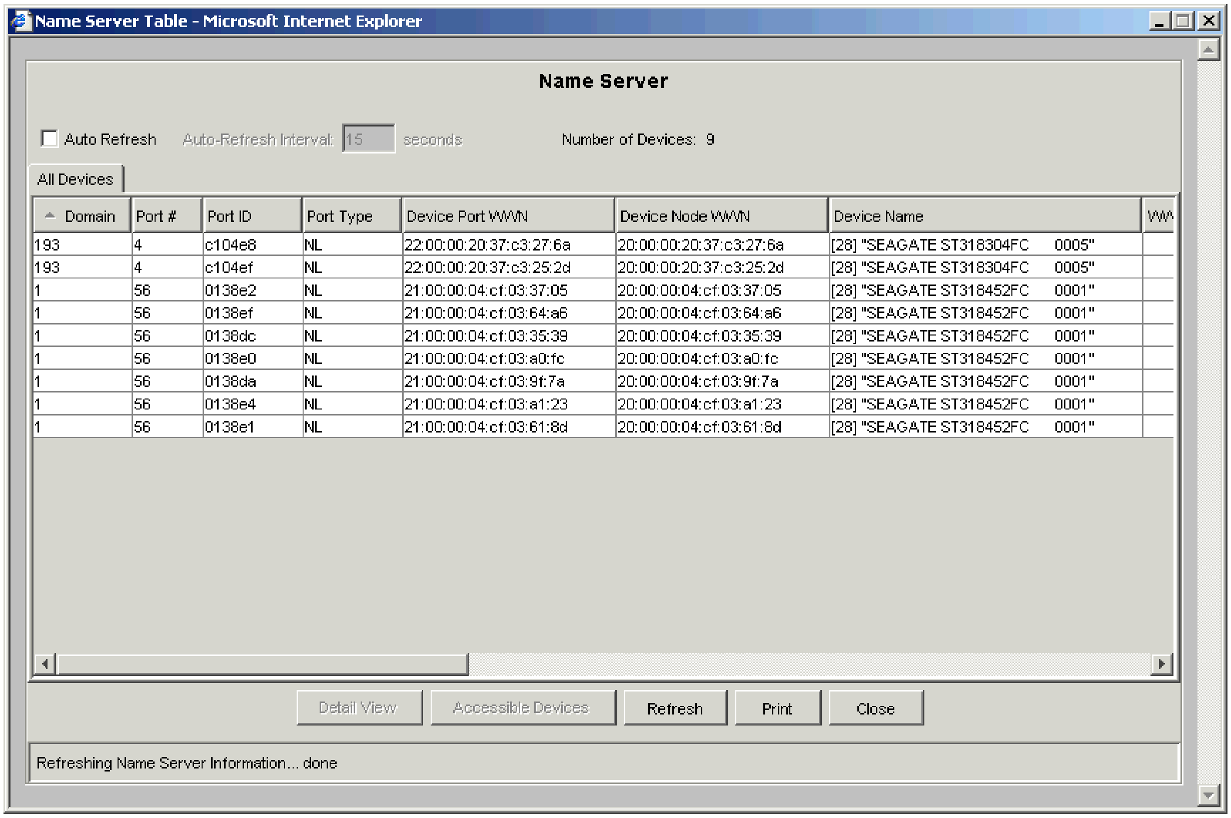
   The Fabric Events window opens.
4. Click **Filter**.

   The Event Filter dialog box opens.
5. Click **Level**.

   The event severity level check boxes are enabled.
6. Select the event levels you want to display.
7. Click **OK**.

   The filter is enabled and the enabled filter type is displayed in the Events Report.

On original page 195, under the heading "Name Server Example," replace original Figure 47, "Name Server Table Window," with the following:



☐ Auto Refresh Auto-Refresh Interval: 15 seconds Number of Devices: 9

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name	WW
193	4	c104e8	NL	22:00:00:20:37:c3:27:6a	20:00:00:20:37:c3:27:6a	[28] "SEAGATE ST318304FC 0005"	
193	4	c104ef	NL	22:00:00:20:37:c3:25:2d	20:00:00:20:37:c3:25:2d	[28] "SEAGATE ST318304FC 0005"	
1	56	0138e2	NL	21:00:00:04:cf:03:37:05	20:00:00:04:cf:03:37:05	[28] "SEAGATE ST318452FC 0001"	
1	56	0138ef	NL	21:00:00:04:cf:03:64:a6	20:00:00:04:cf:03:64:a6	[28] "SEAGATE ST318452FC 0001"	
1	56	0138dc	NL	21:00:00:04:cf:03:35:39	20:00:00:04:cf:03:35:39	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e0	NL	21:00:00:04:cf:03:a0:fc	20:00:00:04:cf:03:a0:fc	[28] "SEAGATE ST318452FC 0001"	
1	56	0138da	NL	21:00:00:04:cf:03:9f:7a	20:00:00:04:cf:03:9f:7a	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e4	NL	21:00:00:04:cf:03:a1:23	20:00:00:04:cf:03:a1:23	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e1	NL	21:00:00:04:cf:03:61:8d	20:00:00:04:cf:03:61:8d	[28] "SEAGATE ST318452FC 0001"	

Refreshing Name Server Information... done

Figure 27: Name Server Table Window

On original pages 195 and 196, under the heading "Name Server Field Descriptions," modify the following information.

In original Table 49, "Name Server Description of Fields and Buttons," add the following rows:

Detail View	Select to display Name Server information for a particular device.
Accessible Devices	Select to display the zone members of a particular device.

On original page 196, replace original Table 50, "Name Server Description of Columns," with the following:

Table 10: Name Server Description of Columns

Column	Description
Domain #	Displays the domain ID of the switch to which the device is connected.
Port #	Displays the number of the switch port to which the device is connected.
Port ID	Displays the port ID of the device (24-bit hexadecimal value).
Port Type	Displays the port type of the device (N for fabric direct-attached port or NL for fabric direct-attached loop port).
Device Port WWN	Displays the World Wide Name of the device port.
Device Node WWN	Displays the World Wide Name of the device node.
Device Name	Displays the symbolic name of the device assigned through the `SCSI INQUIRY` command.
WWN Company ID	Displays the vendor company based on device WWN.
Virtual vs. Physical	Displays the type of device: either virtual or physical.
Host vs. Target	Displays the type of device: either host or target.
Member of Zones	Displays the zones to which this device belongs. This column does not update when the table is refreshed. To view updated zoning information, close and reopen the Name Server Table.
Member of Aliases	Displays the aliases to which this device is assigned, at both device port and node levels.
FC4 Type	Displays the Fibre Channel FC4 layer types supported by the device, such as IP or FCP.
Class Of Service	Displays the Fibre Channel classes of service supported by the device.
Fabric Port Name	Displays the name of the fabric port in use by the device.
Fabric Port WWN	Displays the World Wide Name of the fabric port.
Port IP Address	Displays the IP address of the fabric port.
Hard Address	Displays the hard address of the fabric port.

On original page 197, after the section "Viewing the Name Server," add the following sections:

Displaying Name Server Information for a Device

To display Name Server information for a particular device:

1. Access the Switch Explorer view.
2. Select the **Name Server** icon in the Fabric Tool Bar.

   The Name Server window opens.

3. Select a device from the Domain column and then click **Detail View**.

   The Name Server Information dialog box displays information specific to that device.

Displaying Zone Members of a Device

To display the Zone Members of a particular device:

1. Access the Switch Explorer view.
2. Select the **Name Server** icon in the Fabric Tool Bar.

   The Name Server window opens.

3. Select a device from the Domain column and then click **Accessible Devices**.

   The Zone Accessible Devices dialog box displays accessible zone member information specific to that device.

On original page 204, under the heading "Using the Zone Administration Window," add the following information:

The information in the Zone Admin module is collected from the selected switch. The **Zone Admin** icon is displayed in the Fabric Toolbar only if a Zoning license is installed on the switch. If secure mode is enabled, Zoning can be administered only from the primary FCS switch. If the selected switch has a Zoning license installed but is not the primary switch, the **Zone Admin** icon is displayed in the Fabric Toolbar but not activated.

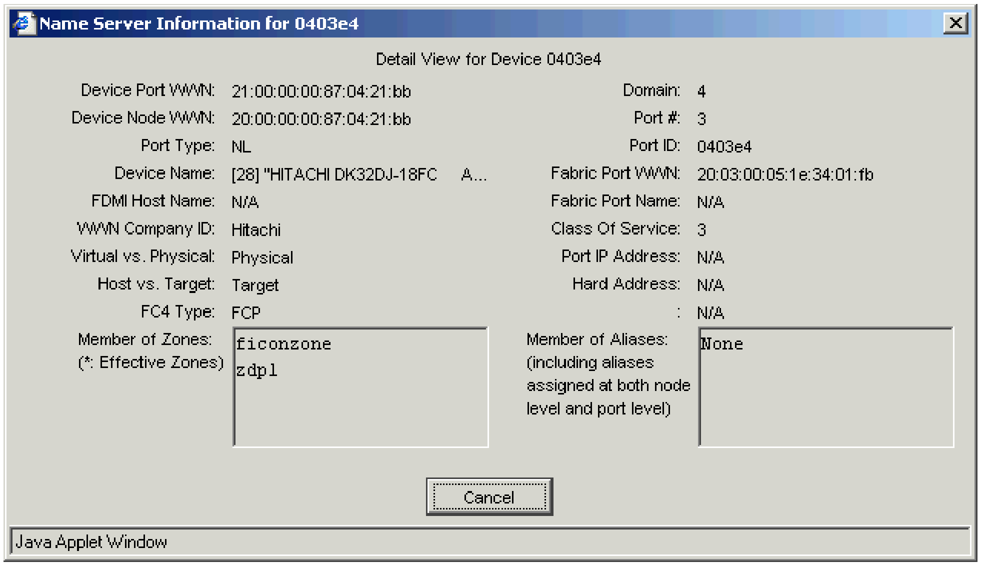
For specific information regarding secure fabrics, refer to the *HP StorageWorks Secure Fabric OS Version 1.0 User Guide*.

When you click the **Zone Admin** icon from the Fabric Toolbar, you must log in as an admin to launch the Zone Admin module. A live snapshot is taken of all the zoning configurations at the time you launch the Zone Admin. To update the information displayed in the Zone Admin module from the switch zone database, see "Refresh Zoning."

Caution: Any changes you make in the Zone Admin module are held in a buffered environment and do *not* update the zoning database until you save them. If you close the Zone Admin module without saving your changes, your changes are lost. To save the buffered changes you make in the Zone Admin module to the zoning database on the switch, see "Saving Changes to an Existing Configuration."

When using a mixed fabric—that is, a fabric containing v4.x, v3.x, and v2.x switches—you should use the most advanced switches to control the fabric. For example, use the v4.x switches as the Primary FCS, the location to perform zoning tasks, and the time server (CLI). You should also use the most recently released firmware on your switches.

In the Zone Admin module, all WWNs also display vendor names. In the member selection lists in the Zone Admin module that display fabric and device information, you can right-click port and device nodes to display which aliases the port or device is a member of. In addition, you can right-click the device nodes and click **View Device Detail** to display the Device Detail view, which launches a window displaying detailed information about the selected device (see Figure 28).



Name Server Information for 0403e4

Detail View for Device 0403e4

Device Port WWN: 21:00:00:00:87:04:21:bb

Device Node WWN: 20:00:00:00:87:04:21:bb

Port Type: NL

Device Name: [28] "HITACHI DK32DJ-18FC A...

FDMI Host Name: N/A

WWN Company ID: Hitachi

Virtual vs. Physical: Physical

Host vs. Target: Target

FC4 Type: FCP

Member of Zones: (*: Effective Zones) ficonzone zdpl

Domain: 4

Port #: 3

Port ID: 0403e4

Fabric Port WWN: 20:03:00:05:1e:34:01:fb

Fabric Port Name: N/A

Class Of Service: 3

Port IP Address: N/A

Hard Address: N/A

: N/A

Member of Aliases: (including aliases assigned at both node level and port level) None

Figure 28: Device Detail View Example

On original page 205, under the heading "About the File Menu," add the following row to original Table 53, "File Menu Options":

View Effective Configuration	Select to view detailed information about the enabled zone configuration.

On original page 205, after the section "About the File Menu," add the following section:

Viewing Detailed Information About the Enabled Zone Configuration

1. Access the Zone Administration window.

   The Zone Configuration in effect at the time you launched the Zone Admin module is identified in the top right corner. This information is updated only when you manually refresh the Zone Admin contents by clicking the **Refresh** icon at the bottom right corner of the Zone Admin window, or when you enable a configuration through the Zone Admin module. If someone changes the effective zone configuration (outside of your Zone Admin session) after you have launched the Zone Admin module, but before you have refreshed the Zone Admin module (by clicking the **Refresh** icon in the bottom right corner), the effective configuration displayed in the upper right corner is not updated.

Caution: Clicking the **Refresh** icon in the lower right corner of the Zone Admin window overwrites all local unsaved zoning changes. If anyone has made any changes to the Zones outside of your Zone Admin session, those changes are applied.

2. Use one of the following methods to identify the most recently effective Zone configuration *without* saving or applying any changes you have made in the Zone Admin module:
   - Click **File** > **View Effective Configuration** in the Zone Admin window.
   - Click the enabled configuration icon in the Zone Admin window.

Both of these actions display the Effective Configuration dialog box. If no zone is enabled, a message is displayed, indicating that there is no active zoning configuration on the switch.

On original page 208, in the section “Adding a WWN in the Zoning Database,” replace the following heading:

Adding a WWN in the Zoning Database

With this heading:

Adding a WWN to Zoning Entities

Add the following step to the procedure:

5. The WWN is added to the Zone Admin buffer and can be used as a member.

On original page 208, in the section “Deleting a WWN in the Zoning Database,” replace the following heading:

Deleting a WWN in the Zoning Database

With this heading:

Deleting a WWN in Zoning Entities

Add the following step to the procedure:

5. The WWN is deleted from the Zone Admin buffer.

On original page 209, in the section “Replacing a WWN in the Zoning Database,” replace the following heading:

Replacing a WWN in the Zoning Database

With this heading:

Replacing a WWN in Zoning Entities

In step 5 of the procedure, replace the following text:

The old WWN is replaced in the Zoning database by the new WWN, including within any Alias or Zone where the old WWN was a member.

With this text:

The old WWN is replaced in the Zone Admin buffer by the new WWN, including within any Alias or Zone where the old WWN was a member.

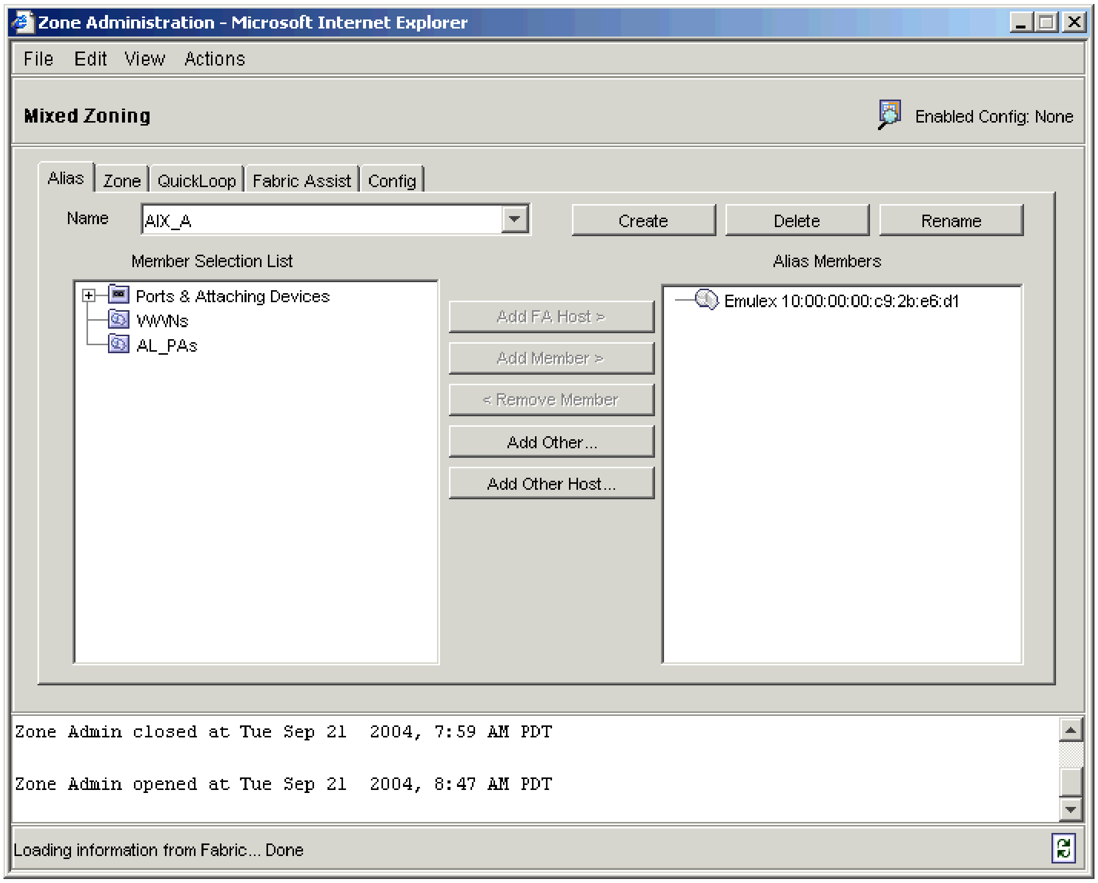
On original page 211, under the heading “Refresh Zoning,” replace the following text in step 2:

This refreshes the Zoning Database.

With this text:

This refreshes the Zone Admin buffer.

On original page 217, under the heading "Alias Tab Example," replace original Figure 51, "Alias Tab in the Zone Administration Window," with the following:



Name: AIX_A

```
Zone Admin closed at Tue Sep 21  2004, 7:59 AM PDT

Zone Admin opened at Tue Sep 21  2004, 8:47 AM PDT
```

Loading information from Fabric... Done

Figure 29: Alias Tab

On original page 221, under the heading "Deleting an Alias," replace the following text in step 5:

The selected Alias is deleted from the zoning database.

With this text:

The selected Alias is deleted from the Zone Admin buffer.

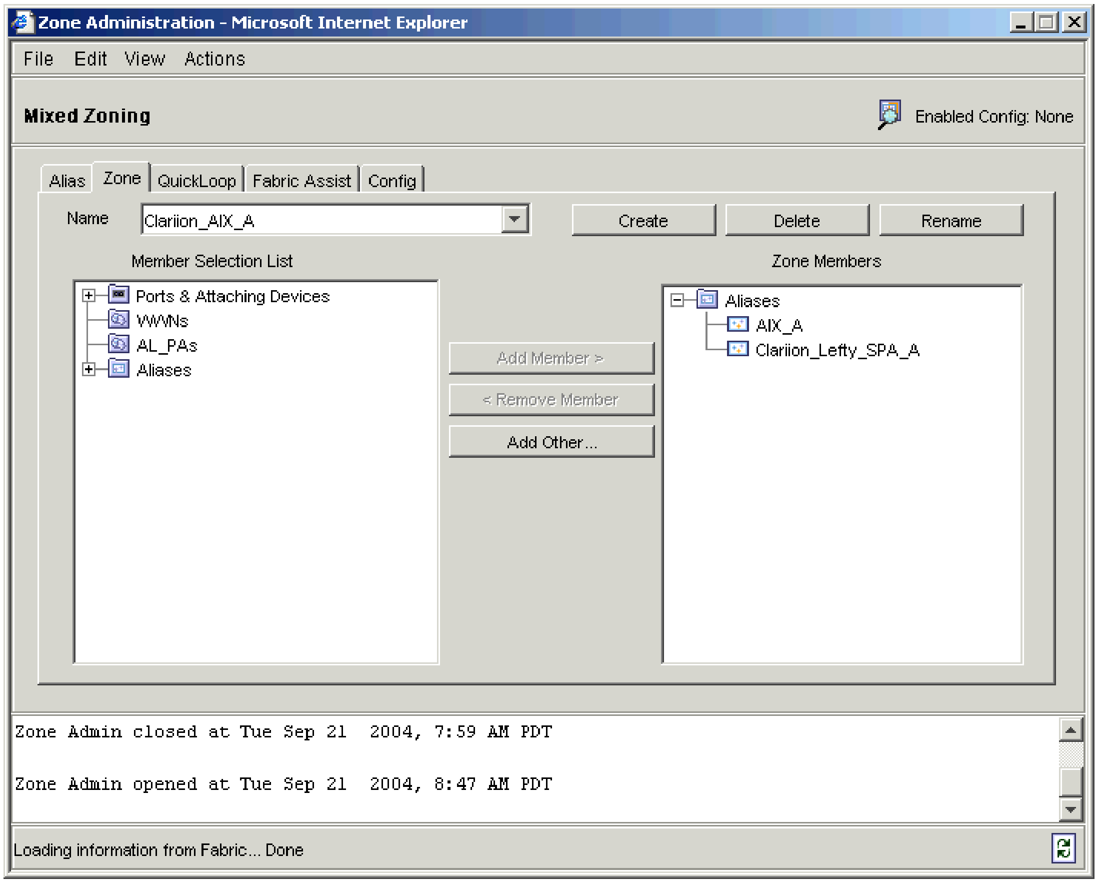
On original page 221, under the heading "Renaming an Alias," replace the following text in step 6:

The Alias is renamed in the zoning database.

With this text:

The Alias is renamed in the Zone Admin buffer.

On original page 223, under the heading "Zone Tab Example," replace original Figure 52, "Zone Tab in the Zone Administration Window," with the following:



Enabled Config: None

Name: Clariion_AIX_A

```
Zone Admin closed at Tue Sep 21  2004, 7:59 AM PDT

Zone Admin opened at Tue Sep 21  2004, 8:47 AM PDT
```

Loading information from Fabric... Done

Figure 30: Zone Tab

On original page 227, under the heading "Deleting an Zone," in step 5, replace the following text:

The selected Zone is deleted from the zoning database.

With this text:

The selected Zone is deleted from the Zone Admin buffer.

On original page 228, under the heading "Renaming a Zone," replace the following text in step 6:

The zone is renamed in the zoning database.

With this text:

The zone is renamed in the Zone Admin buffer.

On original pages 232 and 233, under the heading "Deleting an QuickLoop," in step 5, replace the following text:

The selected QuickLoop is deleted from the zoning database.

With this text:

The selected QuickLoop is deleted from the Zone Admin buffer.

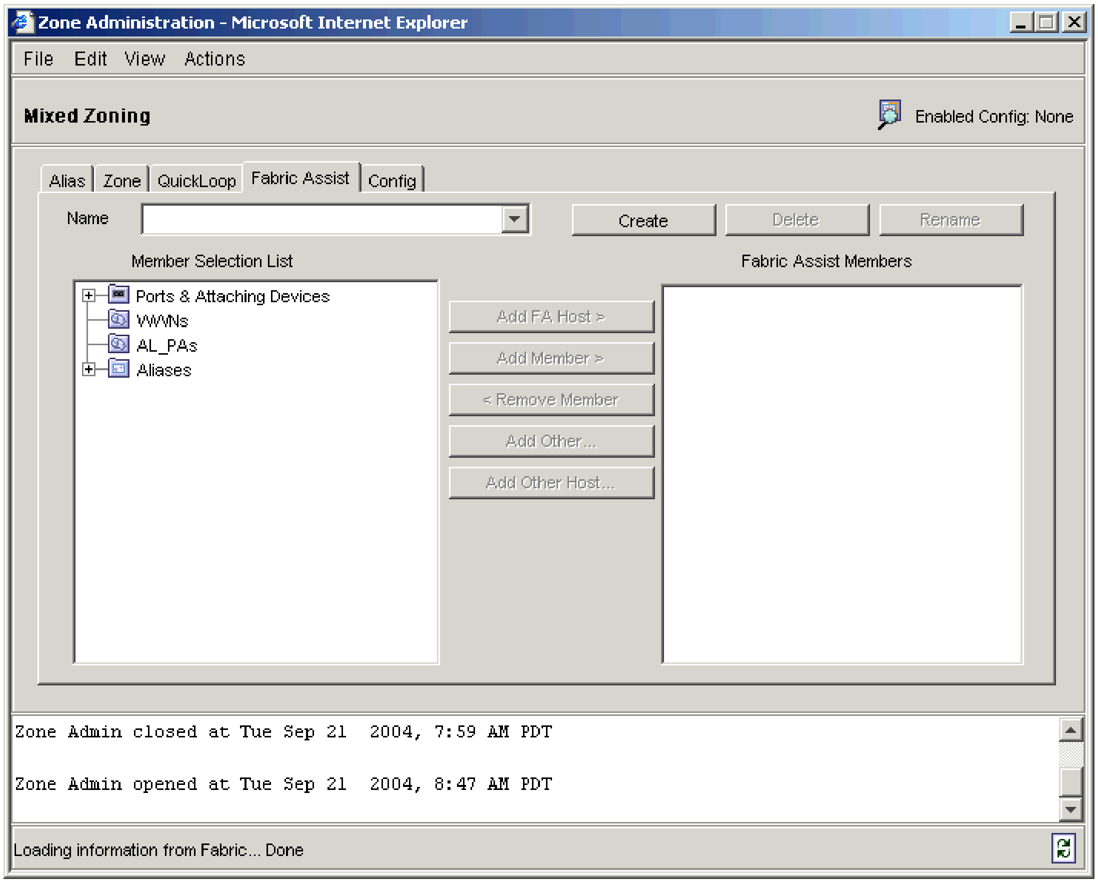
On original page 233, under the heading "Renaming a QuickLoop," replace the following text in step 6:

The QuickLoop is renamed in the zoning database.

With this text:

The QuickLoop is renamed in the Zone Admin buffer.

On original page 234, under the heading "Fabric Assist Example," replace original Figure 54, "Fabric Assist Tab in the Zone Administration Window," with the following:



Enabled Config: None

```
Zone Admin closed at Tue Sep 21  2004, 7:59 AM PDT

Zone Admin opened at Tue Sep 21  2004, 8:47 AM PDT
```

Loading information from Fabric... Done

Figure 31: Fabric Assist Tab

On original page 238, under the heading “Deleting an Fabric Assist Zone,” in step 5, replace the following text:

The selected Fabric Assist Zone is deleted from the zoning database.

With this text:

The selected Fabric Assist Zone is deleted from the Zone Admin buffer.

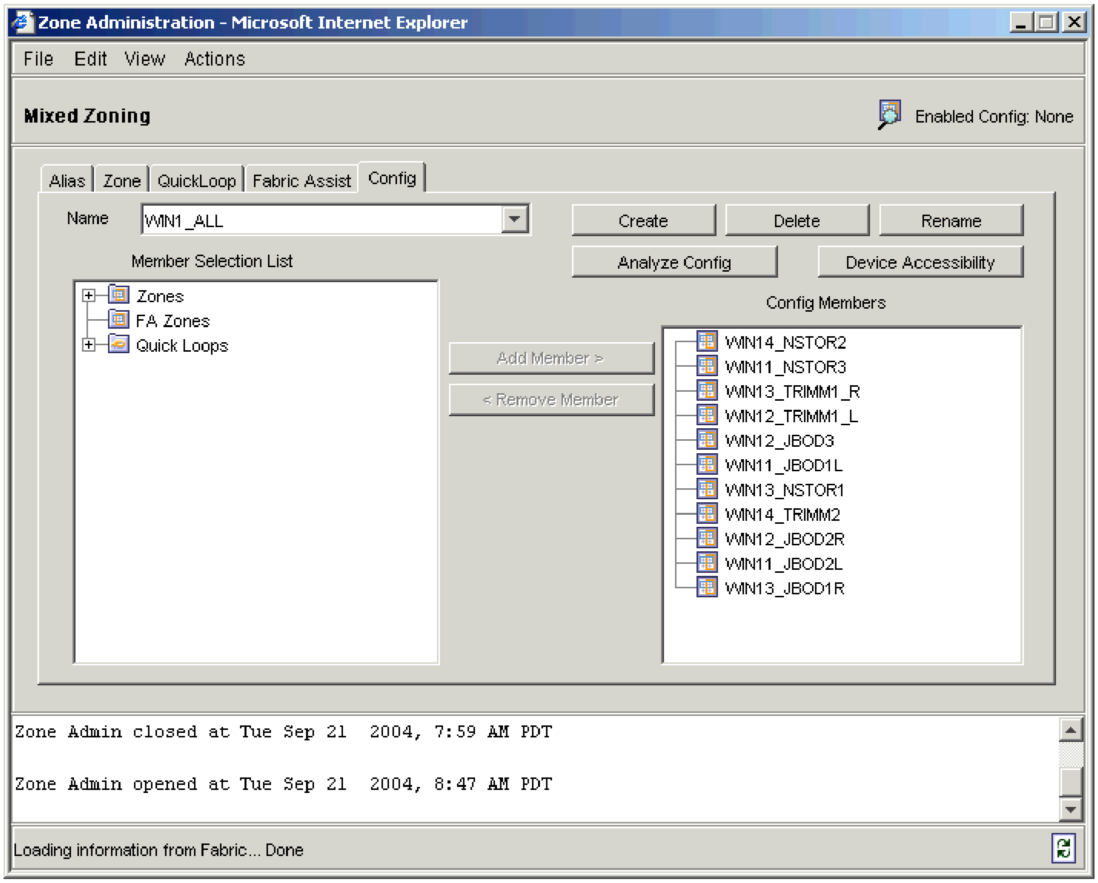
On original page 239, under the heading “Renaming a Fabric Assist Zone,” replace the following text in step 6:

The Fabric Assist Zone is renamed in the zoning database.

With this text:

The Fabric Assist Zone is renamed in the Zone Admin buffer.

On original page 240, under the heading “Config Tab Example,” replace original Figure 55, “Config Tab in the Zone Administration Window,” with the following:



Enabled Config: None

Name: WIN1_ALL

Config Members:

- WIN14_NSTOR2
- WIN11_NSTOR3
- WIN13_TRIMM1_R
- WIN12_TRIMM1_L
- WIN12_JBOD3
- WIN11_JBOD1L
- WIN13_NSTOR1
- WIN14_TRIMM2
- WIN12_JBOD2R
- WIN11_JBOD2L
- WIN13_JBOD1R

```
Zone Admin closed at Tue Sep 21  2004, 7:59 AM PDT

Zone Admin opened at Tue Sep 21  2004, 8:47 AM PDT
```

Loading information from Fabric... Done

Figure 32: Config Tab

On original page 246, after the section "Creating a Configuration Analysis Report," add the following section:

Displaying an Initiator/Target Accessibility

1. Access the Zone Administration window. See "Accessing the Zone Administration Window" for more information.
2. Select the **Config** tab.
3. Select a Configuration to be analyzed from the Name drop-down menu.
4. Click the **Device Accessibility** button.

   The Initiator/Target Accessibility Matrix for Config- Device Selection dialog box opens.
5. Select devices you want displayed in the accessibility matrix; you can select the radio button for all devices in the fabric or for a subset of the devices.

   If you select a subset, you must click the devices from the Select Devices list and then click **Add** to move them to the Evaluate for Accessibility list.
6. Click **OK**.

   The Initiator/Target Accessibility Matrix opens. You can mouse over a target to display the symbolic name of the device. You can click a WWN to launch the device view for that device. You can also right-click the device nodes and click **View Device Detail** to display the Device Detail view, which launches a window displaying detailed information about the selected device.

On original page 267, delete the entire section "Web Tools and Netscape on Solaris."

Zoning version user guide

3

This chapter contains updates to the *HP StorageWorks Zoning Version 3.1.x/4.1.x User Guide*, part number AA-RS26C-TE.

On original page 17, under the heading “License Activation Using Web Tools,” replace the following text:

6. Enter the license key in the **License Key** field and click **Add**. The feature is now activated.

With this text:

6. Click **Add**.
7. Enter the license key in the **License Key** field and click **Add License**. The feature is now activated.

On original page 26, under the heading “Commands to Open a Transaction,” add the following rows to the list:

`zoneObjectCopy`	Copy a zone object.
`zoneObjectExpunge`	Delete a zone object and remove it from member lists of other zone objects.
`zoneObjectRename`	Rename a zone object.

On page 30, under the heading "Detailed Zone Configuration Procedures," add the following:

Table 11 presents zoning database size limitations for various Fabric OS release versions.

Table 11: Zoning Database Limitations

Fabric OS Version	Maximum Database Size (KB)
2.4.0	64
2.5.0	64
2.6.0	96
3.0.0	128
3.1.0	96
3.2.x	256
4.0.0, 4.1.0, 4.2.0	128
4.4.0	256

Note: Zoning databases larger than 96 KB are not supported on SAN Switch 2/8 EL and SAN Switch 2/16 with 16 MB of memory.

Diagnostic and system error messages reference guide

4

This chapter contains updates to the *HP StorageWorks Diagnostic and System Error Messages Version 3.1.x Reference Guide*, part number AA-RUPZA-TE.

The following modules report new (AUTH and SEC) or modified messages in Fabric OS v3.2.x:

- AUTH
- CONFIG
- DIAG
- FABRIC
- MS
- SEC

AUTH-AUTHCHANGE

Message

```
<timestamp>
INFO AUTH-AUTHCHANGE, 4, <text message>
```

Probable Cause

The AUTH database was modified. The *`text message`* can display the following information:

- Secret database was successfully updated.
- Secret database was successfully removed.

Recommended Action

Verify that this change was intended.

Severity

INFO

AUTH-AUTHCFGCHANGE

Message

```
<timestamp>
INFO AUTH-AUTHCFGCHANGE, 4, <text message>
```

Probable Cause

The authentication type or the group type was modified. The *`text message`* can display the following information:

- Authentication type was successfully set to `fcap`, `dhchap`, or `fcap, dhchap`.
- Group type was successfully set to `0, 1, 2, 3, 4` or `0,1,2,3,4`.

Recommended Action

Verify that this change was intended. If the change was intended, no action is required.

Severity

INFO

AUTH-AUTHCFGERROR

Message

```
<timestamp>
ERROR AUTH-AUTHCFGERROR, 2, <text message>
```

Probable Cause

The authentication type or the group type was not set. The *`text message`* can display the following information:

- Failed to set authentication to either `fcap`, `dhchap`, or `fcap, dhchap.`
- Failed to set group type to either `0, 1, 2, 3, 4` or `0,1,2,3,4`.

Recommended Action

Usually this problem is transient. Retry the command.

If the command fails consistently, copy the message, collect switch information using the `supportshow` command, and contact your switch service provider.

Severity

ERROR

AUTH-AUTHINFO

Message

```
<timestamp>
INFO AUTH-AUTHINFO, 4, <text message>
```

Probable Cause

An INFO-level authentication failure occurred. The *`text message`* can display the `Failed to create a timer for authentication` message.

Recommended Action

Usually this problem is transient. Reinitialize authentication by issuing the `switchdisable` and `switchenable` commands or the `portdisable` and `portenable` commands.

Severity

INFO

AUTH-AUTHWARN

Message

```
<timestamp>
WARNING AUTH-AUTHWARN, 3, <text message>
```

Probable Cause

A WARNING-level authentication failure occurred. The *`text message`* can display the following information:

- Failed to allocate memory for various authentication payloads or messages.

Recommended Action

Usually this problem is transient. Reinitialize authentication by issuing `switchdisable` and `switchenable` commands or the `portdisable` and `portenable` commands.

If the command fails consistently, copy the message, collect switch information using the `supportshow` command, and contact your switch service provider.

Severity

WARNING

AUTH-AUTHERROR

Message

```
<timestamp>
ERROR AUTH-AUTHERROR, 2, <text message>
```

Probable Cause

An ERROR-level authentication failure occurred. The *`text message`* displays more information about the failure that occurred.

General authentication errors:

- Authentication is rejected because the other side does not support authentication or a required protocol.
- Internal error due to data mismatch or corruption.
- Various error types that relate to authentication configuration file such as empty file, corruption file, or nonexistent file.
- Failed to get information for authentication entry such as port or switch.
- Failed to get security license.
- Failed to validate switch or port name.
- Disabled port due to unauthorized switch that is not configured in the SCC policy.

Specific FCAP/SLAP authentication errors:

- Failed to retrieve switch certificate.
- Failed to sign data for FCAP/SLAP authentication messages.
- Incorrect length or content in the FCAP/SLAP authentication payload, such as nonce length, signature length, or certificate length.
- Failed to verify different types of authentication messages (for example, certificate, nonce, or signature data) for FCAP/SLAP authentication protocol.

Specific DH-CHAP authentication errors:

- Failed to update/remove secret database when using `secAuthSecret` command.
- Failed to retrieve secret value.
- Failed to generate various values for DH-CHAP authentication messages, such as DH group, hash value, challenge message, or response value.
- Incorrect length or content in the authentication payload, such as challenge length, DH group length, hash list length, or response length.
- Failed to verify different types of authentication messages (for example, reply or success) for DH-CHAP authentication protocol.

Recommended Action

For a security license error, make sure that the security license is properly installed, using the `licenseshow` command. Reinstall the license, if necessary, using the `licenseadd` command.

For an unauthorized switch in the SCC policy, add the switch WWN to the SCC policy, using the `secpolicyadd` command.

For a certificate retrieve error, make sure the switch certificate is properly installed, using the `pkishow` command. Reinstall the certificate, if necessary, using the `pkicert` command.

For a secret retrieve error, make sure that the secret values are properly set. Reset the secret values using the `secauthsecret` command.

For other internal errors (for example, bad payload, incorrect field length, or invalid object), this might be a transient error. Use the `switchdisable` and `switchenable` commands or `portdisable` and `portenable` commands to determine whether the problem is consistent.

Other errors (for example, invalid nonce, signature, reply message, or response value) might indicate that an invalid entity is trying to connect to the switch. Check the connection port to verify that there is no security attack. Otherwise, use the `switchdisable` and `switchenable` commands or `portdisable` and `portenable` commands to determine whether the problem is consistent.

Severity

ERROR

CONFIG-PIDCHANGE_EXTENDED_EDGE

Message

```
<timestamp>

WARNING CONFIG-PIDCHANGE_EXTENDED_EDGE, 3, Switch PID format changed to
Format 2 ('Extended Edge PID Format').
```

Probable Cause

The PID format for the fabric was changed to Format 2, extended-edge PID. For more information on PID format, refer to the *HP StorageWorks Fabric OS Procedures Version 3.1.x/4.1.x User Guide*.

Recommended Action

This message is for information purposes only. The entire fabric must be configured with the same PID format or the fabric segments.

Severity

WARNING

DIAG-BADINT

Message

```
<timestamp>
CRITICAL DIAG-BADINT, 1, <test name>, pass <number>,
Pt<port information> got interrupt,
int_status=0x<int number> when not expecting one,
Err# <error code>
```

Probable Cause

A port received an unexpected interrupt. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` or the `cmitest` command. The *`error code`* value is for internal use only.

Recommended Action

For the HP StorageWorks SAN Switch 2/16, replace the motherboard FRU.

For the HP StorageWorks SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-BUS_TIMEOUT

Message

```
<timestamp>
CRITICAL DIAG-BUS_TIMEOUT, 1, <test name>,
Pt<port information> BTO accessing <Register Name> Register at Address
<address>,
Err# <error code>
```

Probable Cause

The ASIC register or ASIC SRAM did not respond to an ASIC data access. This usually indicates an ASIC failure. This message is generated by the `portregtest` or the `sramretentiontest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CAMFLTR

Message

```
<timestamp>
CRITICAL DIAG-CAMFLTR, 1, <test name>, pass <number>,
Pt<port info> Failed Filter Test (test=<test number>, match:<cam type>),
filter <hit | nhit> on <actual filter number>(sb:<expected filter number>)
action type: <actual action>(sb:<expected action>)
Err# <error code>
```

Probable Cause

The ASIC internal logic failed. This usually indicates an ASIC failure. This message is generated by the `filtertest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CAMINIT

Message

```
<timestamp>
CRITICAL DIAG-CAMINIT, 1, <test name>, pass <number>,
Pt<port information> Failed to Init: <additional message>,
Err# <error code>
```

Probable Cause

A port failed to initialize due to one of the following reasons:

- Switch is not disabled.
- Diagnostic queue is absent.
- Malloc failed.
- Chip is not present.
- Port is not in loopback mode.
- Port is not active.
- There was a software operational setup error or motherboard failure.
- There occurred a retry, reboot, or replacement of motherboard assembly.

This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `camtest` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CAMSID

Message

```
<timestamp>
CRITICAL DIAG-CAMSID, 1, <test name>, pass <number>,
Pt<port information> Failed SID [No] translation test,
SID received is 0x<Actual SID>, SID transmitted 0x<expected SID>,
Err# <error code>
```

Probable Cause

The ASIC failed the SID NO translation test. This usually indicates an ASIC failure. This message is generated by the `camtest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CAMSTAT

Message

```
<timestamp>
CRITICAL DIAG-CAMSTAT, 1, <test name>, pass <number>,
Pt<port information> Failed ALI: <idx>, ALPA: 0x<ALPA number> counter:
<cnt>
Err# <error code>
```

Probable Cause

The ASIC improperly counted the number of frames with CRC errors. This usually indicates an ASIC failure. This message is generated by the `statisticstest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CLEAR_ERR

Message

```
<timestamp>
INFO DIAG-CLEAR_ERR, 3, Pt<port information> Diagnostics Error Cleared
Err# <error code>
```

Probable Cause

The port diag error flag (`OK` or `BAD`) is cleared. The *`error code`* value is for internal use only.

Recommended Action

No action is required.

Severity

INFO

DIAG-CMBISRF

Message

```
<timestamp>
CRITICAL DIAG-CMBISRF, 1, <test name>, pass <number>,
Pt<port information> BISR,BIST Self-Test Failed,
RAMs fail bitmap: is 0x<actual value> sb 0x<expected value> er 0x<err
value>,
Err# <error code>
```

Probable Cause

The ASIC central memory SRAMs did not complete the BISR within the timeout period. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMBISRTO

Message

```
<timestamp>
CRITICAL DIAG-CMBISRTO, 1, <test name>, pass <number>,
Pt<port information> BISR,BIST Timed Out,
RAMs done bitmap: is 0x<actual value> sb 0x<expected value> er 0x<err
value>,
Err# <error code>
```

Probable Cause

The ASIC central memory SRAMs did not complete the BISR within the timeout period. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMERRPTN

Message

```
<timestamp>
CRITICAL DIAG-CMERRPTN, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info> Offs <offset value> <err
str> detected at wrong port,
Checking Pt<check pt>: is <actual value> sb <expected value>,
Err# <error code>
```

Probable Cause

A problem was detected at the wrong port. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMERRTYPE

Message

```
<timestamp>
CRITICAL DIAG-CMERRTYPE, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info> Offs <offset value> Wrong
Err Type,
Checking Pt<check pt>: is <actual value> (<err str>) sb <expected value>
(<err str>),
Err# <error code>
```

Probable Cause

The port got the wrong CMEM error type. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMICKSUM

Message

```
<timestamp>
CRITICAL DIAG-CMICKSUM, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info>: Pt<src/dst pt> Failed
[good/bad/not target] Cksum Test,
cmi_err bit6 is <actual value> sb <expeted value>, bad msg is from <CMI
bit>,
Err# <error code>
```

Probable Cause

The CMI message received failed. This usually indicates an ASIC or motherboard failure. This message is generated by the `cmitest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMIDATA

Message

```
<timestamp>
CRITICAL DIAG-CMIDATA, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info>: RX Data is <actual value>
sb <expected value> er 0x<err value>,
Err# <error code>
```

Probable Cause

The CMI data received did not match data transmitted. This usually indicates an ASIC or motherboard failure. This message is generated by the `cmitest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMIINVCAP

Message

```
<timestamp>
CRITICAL DIAG-CMIINVCAP, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info>: Pt<fail port> erroneously
got CMI Capture Flag (bit31 is 1),
Err# <error code>
```

Probable Cause

The ASIC unintentionally got a CMI capture flag. This usually indicates an ASIC or motherboard failure. This message is generated by the `cmitest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMINOCAP

Message

```
<timestamp>
CRITICAL DIAG-CMINOCAP, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info>: RX Pt<fail port> Failed to
get CMI Capture Flag (bit31 is 0),
Err# <error code>
```

Probable Cause

The CMI recipient ASIC failed to get a CMI capture flag. This usually indicates an ASIC or motherboard failure. This message is generated by the `cmitest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMISA1

Message

```
<timestamp>
CRITICAL DIAG-CMISA1, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info>: TX Pt<fail port> CMI
Self-Test Start bit30 s-a-1,
Err# <error code>
```

Probable Cause

An attempt to send a CMI message from one ASIC to another failed. This usually indicates an ASIC failure. This message is generated by the `cmitest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-CMNOBUF

Message

```
<timestamp>
CRITICAL DIAG-CMNOBUF, 1, <test name>, pass <number>,
Pt<port information> No More Buffers,
Err# <error code>
```

Probable Cause

The port could not get any buffers. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-DATA

Message

```
<timestamp>
CRITICAL DIAG-DATA, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info>: RX Data is 0x<actual value>
sb 0x<expected value> er 0x%<err value>,
Err# <error code>
```

Probable Cause

The payload received by a port did not match the payload transmitted. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `crossporttest` or `portloopbacktest` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-ERRSTAT (2LONG)

Message

```
<timestamp>
CRITICAL DIAG-ERRSTAT (2LONG), 1, <test name>, pass <number>,
Pt<port information> FrmTooLong Error Counter is <number> sb 0,
Err# <error code>
```

Probable Cause

The Port Error Statistics counter is nonzero, which means that a `Frame too long` error was detected when receiving frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-ERRSTAT (BADEOF)

Message

```
<timestamp>
CRITICAL DIAG-ERRSTAT (BADEOF), 1, <test name>, pass <number>,
Pt<port information> BadEOF Error Counter is <number> sb 0,
Err# <error code>
```

Probable Cause

The Port Error Statistics counter is nonzero, which means that a `Bad end of file` error was detected when receiving frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-ERRSTAT (BADORD)

Message

```
<timestamp>
CRITICAL DIAG-ERRSTAT (BADORD), 1, <test name>, pass <number>,
Pt<port information> BadOrdSet Error Counter is <number> sb 0,
Err# <error code>
```

Probable Cause

The Port Error Statistics counter is nonzero, which means that a `Bad symbol on fiber-optic cable` error was detected when receiving frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-ERRSTAT (CRC)

Message

```
<timestamp>
CRITICAL DIAG-ERRSTAT (CRC), 1, <test name>, pass <number>,
Pt<port information> CRC_err Error Counter is <number> sb 0,
Err# <error code>
```

Probable Cause

The Port Error Statistics counter is nonzero, which means that a `Cyclic redundancy check on frame failed` error was detected when receiving frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-ERRSTAT (DISCC3)

Message

```
<timestamp>
CRITICAL DIAG-ERRSTAT (DISCC3), 1, <test name>, pass <number>,
Pt<port information> DiscC3 Error Counter is <number> sb 0,
Err# <error code>
```

Probable Cause

The Port Error Statistics counter is nonzero, which means that a `Discarded Class 3 frames` error was detected when receiving frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-ERRSTAT (ENCIN)

Message

```
<timestamp>
CRITICAL DIAG-ERRSTAT (ENCIN), 1, <test name>, pass <number>,
Pt<port information> Enc_in Error Counter is <number> sb 0,
Err# <error code>
```

Probable Cause

The Port Error Statistics counter is nonzero, which means that an `Encoding error, inside frame` error was detected when receiving frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-ERRSTAT (ENCOUT)

Message

```
<timestamp>
CRITICAL DIAG-ERRSTAT (ENCOUT), 1, <test name>, pass <number>,
Pt<port information> Enc_out Error Counter is <number> sb 0,
Err# <error code>
```

Probable Cause

The Port Error Statistics counter is nonzero, which means that an `Encoding error, outside frame` error was detected when receiving frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-ERRSTAT (TRUNC)

Message

```
<timestamp>
CRITICAL DIAG-ERRSTAT (TRUNC), 1, <test name>, pass <number>,
Pt<port information> TruncFrm Error Counter is <number> sb 0,
Err# <error code>
```

Probable Cause

The Port Error Statistics counter is nonzero, which means that a `Truncated frame` error was detected when receiving frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-INIT

Message

```
<timestamp>
CRITICAL DIAG-INIT, 1, <test name>, pass <number>,
Pt<port information><speed> Failed to go active after initialization,
Err# <error code>
```

Probable Cause

The port failed to go active in the loopback mode requested. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `crossporttest`, `portloopbacktest`, or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-INTNIL

Message

```
<timestamp>
CRITICAL DIAG-INTNIL, 1, <test name>, pass <number>,
Pt<port information> Failed to get CMI Error (interrupt),
Err# <error code>
```

Probable Cause

The ASIC failed to get a CMI error (interrupt). This usually indicates an ASIC failure. This message is generated by the `cmitest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-INTNOTCLR

Message

```
<timestamp>
CRITICAL DIAG-INTNOTCLR, 1, <test name>, pass <number>,
Pt<port information> Offs <offset value> CMEM_ERR int bit could not be
cleared,
Err# <error code>
```

Probable Cause

The interrupt bit could not be cleared. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-LCMEM

Message

```
<timestamp>
CRITICAL DIAG-LCMEM, 1, <test name>, pass <number>,
Pt<port information> Data Wr/Rd,
bNum 0x<buf number> bLine 0x<line number> lineOffs 0x<offset number> is
<actual value> sb <expected value> er <error value>,
Err# <error code>
```

Probable Cause

The data read from the central memory location did not match data previously written into the same location. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` and `cmemretentiontest` commands. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-LCMEMTX

Message

```
<timestamp>
CRITICAL DIAG-LCMEMTX, 1, <test name>, pass <number>,
Pt<source port info>-Pt<destination port info> Read Via TX Path,
Word <word number> is <actual value> sb <expected value> er <error value>,
Err# <error code>
```

Probable Cause

A central memory transmit path failure occurred: ASIC 1 failed to read ASIC 2 using the transmit path. This usually indicates a motherboard failure. This message is generated by the `centralmemorytest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-LCMRS

Message

```
<timestamp>
CRITICAL DIAG-LCMRS, 1, <test name>, pass <number>,
Pt<port information> Read Short: is <actual value> bytes sb <expected
value>,
Starting from <starting register>,
Err# <error code>
```

Probable Cause

A central memory read short occurred; that is, a number of bytes were requested but not received. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` and `cmemretentiontest` commands. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-LCMTO

Message

```
<timestamp>
CRITICAL DIAG-LCMTO, 1, <test name>, pass <number>,
Pt<port information> CMEM Timeout during a [read/write],
mem_ctl's MEM_RUNNING bit 0 Stuck High,
Err# <error code>
```

Probable Cause

A central memory timeout occurred: data transfer initiated did not complete within the timeout period. This usually indicates an ASIC failure. This message is generated by the `centralmemorytest` and `cmemretentiontest` commands. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-MEMNULL

Message

```
<timestamp>
CRITICAL DIAG-MEMNULL, 1, <test name>,
Failed to malloc memory,
Err# <error code>
```

Probable Cause

The ASIC failed to allocate memory. This usually indicates a motherboard failure. This message is generated by the `ramtest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-MEMORY

Message

```
<timestamp>
CRITICAL DIAG-MEMORY, 1, <test name>,
Memory Error, Address <address value> is 0x<actual value> sb 0x<expected
value> er 0x<err value>,
Err# <error code>
```

Probable Cause

The data read from the RAM location did not match previously written data into the same location. This usually indicates a CPU RAM failure. This message is generated by the `ramtest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-MEMSZ

Message

```
<timestamp>
CRITICAL DIAG-MEMSZ, 1, <test name>,
Memory size to test <= 0,
memFindMax = <max mem size> and N_UNTESTED_RAM = <number>,
Err# <error code>
```

Probable Cause

The memory size to be tested is less than or equal to 0. This usually indicates a motherboard failure. This message is generated by the `ramtest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-NOSEGMENT

Message

```
<timestamp>
CRITICAL DIAG-NOSEGMENT, 1, <test name>,
Pt<port info><speed> Failed to segment,
Please check cables,
Err# <error code>
```

Probable Cause

The port failed to go into loopback mode. This message usually indicates improper cable connections. This message is generated by the `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Verify cable connections. Reseat the SFPs and cables and then reexecute the test. Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary.

Severity

CRITICAL

DIAG-PORTABSENT

Message

```
<timestamp>
CRITICAL DIAG-PORTABSENT, 1, <test name>, pass <number>,
Pt<port info> is not present, cannot run test,
Err# <error code>
```

Probable Cause

The port is not present. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-PORTDIED

Message

```
<timestamp>
CRITICAL DIAG-PORTDIED, 1, DIAG-PORTDIED
<test name>, pass <number>,
Pt<port info><speed> Was Active but Went Inactive (Offline),
Err# <error code>
```

Probable Cause

The port was in loopback mode and then went inactive. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `crossporttest`, `portloopbacktest`, or `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-PORTM2M

Message

```
<timestamp>
CRITICAL DIAG-PORTM2M, 1, <test name>,
Pt<port info> Port M->M Connection not allowed,
Err# <error code>
```

Probable Cause

The port is connected to itself (self-loopback). This port M-to-port M connection is not allowed by the test. This message usually indicates improper cable connections. This message is generated by the `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Reconnect port (M) to a different port (N) and reexecute the test.

Severity

CRITICAL

DIAG-PORTSTOPPED

Message

```
<timestamp>
CRITICAL DIAG-PORTSTOPPED, 1, <test name>, <number> nMegs,
Pt<port info> No Longer Transmitting, FTX Counter Stuck at <count>,
Err# <error code>
```

Probable Cause

The port is no longer transmitting, as indicated by the number of frames transmitted counter being stuck at N frames. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `spinsilk` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-PORTWRONG

Message

```
<timestamp>
CRITICAL DIAG-PORTWRONG, 1, <test name>, pass <number>,
Frame Received at Wrong Port: is Pt<actual port> sb Pt<expected port>,
Err# <error code>
```

Probable Cause

The frame was erroneously received by port M instead of the intended port N. This usually indicates an ASIC failure. This message is generated by the `portloopbacktest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-POST_SKIPPED

Message

```
<timestamp>
WARNING DIAG-POST_SKIPPED, 4, Skipped POST tests: assuming all ports are
healthy,
Err# <error code>
```

Probable Cause

The POST was not executed on the last boot. The *`error code`* value is for internal use only.

Recommended Action

No action is required.

Severity

WARNING

DIAG-REGERR

Message

```
<timestamp>
CRITICAL DIAG-REGERR, 1, <test name>,
Pt<port info> "<register name>" is <actual value> sb <expected> er <err
value>,
offs <offset value> phy <physical address> msk <mask value>,
Err# <error code>
```

Probable Cause

The data read from an ASIC register or ASIC SRAM did not match data previously written into the same location. This usually indicates an ASIC failure. This message is generated by the `portregtest` or the `sramretentiontest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-REGERR_UNRST

Message

```
<timestamp>
CRITICAL DIAG-REGERR_UNRST, 1, <test name>,
Pt<port info> failed to unreset despite <number> retries,
lli_ctl is <actual value> sb 90000, port_config is <actual value> sb 0,
Err# <error code>
```

Probable Cause

The port failed to un-reset. This usually indicates an ASIC failure. This message is generated by the `portregtest` or the `sramretentiontest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-STATS (C3FRX)

Message

```
<timestamp>
CRITICAL DIAG-STATS (C3FRX), 1, <test name>, pass <number>,
Pt<port info> Cl3FrmRx Counter Wrong, is <actual value> sb <expected
value>,
Err# <error code>
```

Probable Cause

The port counter value did not match the number of frames actually transmitted. In this case, `Cl3FrmRx` equals the number of Class 3 frames received. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-STATS (FRX)

Message

```
<timestamp>
CRITICAL DIAG-STATS (FRX), 1, <test name>, pass <number>,
Pt<port info> FramesRx Counter Wrong, is <actual value> sb <expected
value>,
Err# <error code>
```

Probable Cause

The port counter value did not match the number of frames actually transmitted. In this case, `FramesRx` equals the number of frames received. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-STATS (FTX)

Message

```
<timestamp>
CRITICAL DIAG-STATS (FTX), 1, <test name>, pass <number>,
Pt<port info> FramesTx Counter Wrong, is <actual value> sb <expected
value>,
Err# <error code>
```

Probable Cause

The port counter value did not match the number of frames actually transmitted. In this case, `FramesTx` equals the number of frames transmitted. This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. This message is generated by the `portloopbacktest` command. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-TBRAM_DEC_RWTEST

Message

```
<timestamp>
CRITICAL DIAG-TBRAM_DEC_RWTEST, 1, <test name>, pass <number>,
Pt<port info> Failed Turbo RAM dec r/w test:
phy=0x<address> wrd cnt=<cnt> inc size=<size> bytes
rpt=0x<actual pattern> wpt=0x<expected pattern> msk=0x<mask value>
Err# <error code>
```

Probable Cause

The ASIC internal registers failed the read-modify-write operation. This usually indicates an ASIC failure. This message is generated by the `turboramtest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-TBRAM_INC_RWTEST

Message

```
<timestamp>
CRITICAL DIAG-TBRAM_INC_RWTEST, 1, <test name>, pass <number>,
Pt<port info> Failed TurboRAM inc r/w test:
phy=0x<address> wrd cnt=<cnt> inc size=<size> bytes
rpt=0x<actual pattern> wpt=0x<expected pattern> msk=0x<mask value>
Err# <error code>
```

Probable Cause

The ASIC internal registers failed the read-modify-write operation. This usually indicates an ASIC failure. This message is generated by the `turboramtest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-TBRAM_WTEST

Message

```
<timestamp>
CRITICAL DIAG-TBRAM_WTEST, 1, <test name>, pass <number>,
Pt<port info> Failed TurboRAM write test:
phy=0x<address> wrd cnt=<cnt> inc size=<size> bytes
wpat=0x<write pattern>
Err# <error code>
```

Probable Cause

The ASIC internal registers failed on a write operation. This usually indicates an ASIC failure. This message is generated by the `turboramtest` command. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-TIMEOUT

Message

```
<timestamp>
CRITICAL DIAG-TIMEOUT, 1, <test name>, pass <number>,
Pt<port info> Receive Timeout,
Err# <error code>
```

Probable Cause

For `portloopbacktest` and `crossporttest`:

```
Port failed to receive frame within timeout period.
```

For `centralmemorytest`:

```
Port failed to detect an interrupt within the timeout period.
```

This can be caused by a faulty cable or deteriorated SFP. It can also indicate more serious problems in the motherboard or ASIC. The *`error code`* value is for internal use only.

Recommended Action

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. If the problem persists:

- For the SAN Switch 2/16, replace the motherboard FRU.
- For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

DIAG-XMIT

Message

```
<timestamp>
CRITICAL DIAG-XMIT, 1, <test name>, pass <number>,
Pt<port info> Cannot Transmit Frame: <ftx function> returns <error>,
Err# <error code>
```

Probable Cause

The port failed to transmit a frame. This usually indicates an ASIC failure. This message is generated by the `camtest`, `portloopbacktest`, and `spinsilk` commands. The *`error code`* value is for internal use only.

Recommended Action

For the SAN Switch 2/16, replace the motherboard FRU.

For the SAN Switch 2/8 EL, replace the entire switch.

Severity

CRITICAL

FABRIC-RECONFIG

Message

```
<timestamp>
INFO FABRIC-RECONFIG, 4, fabric: <reason>
```

Probable Cause

The fabric has reconfigured due to an offline port. The *`reason`* can be one of the following:

`Fabric Merge`	Merging two fabrics
`Own ID Rcvd`	A subordinate switch received an EFP or EFP ACC that has a payload error, listing this switch as being the principal switch.
`Fabric Segment`	Principal port became segmented.
`Offline`	Principal port went offline.
`Unconfirmed domain`	Switch was not able to get a domain ID. RDI ACC was never received.
`Rcv BF`	Received Build Fabric (BF) command.
`HA: At F2 State`	According to the Fibre Channel specification, F2 is defined as the principal switch selection. If a failover occurs at this time, the switch is forced to restart principal switch selection.
`HA: No Upstream`	After failover, the newly active fabric reboots as a subordinate, but there is no upstream fabric.
`HA: bad EFP resp`	Received an invalid EFP response.
`HA: RJT EFP resp`	Received an EFP reject response in which this EFP was used for verifying the neighbor's domain list as part of fabric warm-start recovery. A reject occurs if the neighbor is reconfiguring or the neighbor's port is in a bad state.
`HA: DLST EFP resp`	Received an EFP accept response with a different domain list.
`HA: PPRI EFP resp`	Received an EFP accept response in which the response has a different principal switch priority number.
`HA: PWWN EFP resp`	Received an EFP accept response in which the response has a different principal switch World Wide Name.
`HA: MAX EFP resp`	An EFP to a neighbor failed to respond, and the fabric reached its maximum retry count for this neighboring switch.
`HA: Can't Snd EFP`	Was not able to send an EFP.
`HA: Offline`	A principal port went offline during the fabric daemon's warm-start recovery.
`Principal Selection Mode`	The user has run the `fabricprincipal` command, forcing a fabric rebuild.

`D-list conflict`	The principal switch received a domain list that contains more domains than what the principal switch has already assigned.

Recommended Action

If the reconfiguration was unplanned, check for problems with the specified port. Some troubleshooting tasks consist of:

- Verifying that the port was not disabled, using the `portshow` command
- Verifying that the port is cabled correctly
- Verifying that the SFP has not deteriorated

Refer to the *Fibre Channel Standard FC-SW3*, Chapters 6 and 7, for more information on fabric initialization.

Severity

INFO

MS-CT_REQUEST_FAIL

Message

```
<timestamp>

WARNING MS-CT_REQUEST_FAIL, 3, MS CT request failure for domain <domain>
(cmd=0xF004, code=0xFFFFFFFF)
```

Probable Cause

The management server (MS) received an invalid common transport (CT) response from switch ***`domain`***. MS expects either a CT accept IU or a reject IU; the management server received neither response, which violates the Fibre Channel Generic Services (FS-GS) specification.

Recommended Action

Check the integrity of the FC switch at the specified domain. It is not sending correct MS information as defined by the FC-GS standard.

Severity

WARNING

SEC-ACCT, Added

Message

```
<timestamp>
INFO SEC-ACCT, 4, <message> Added account <user name> with <role name>
authorization
```

Probable Cause

The specified new account was created.

Recommended Action

No action is required.

Severity

INFO

SEC-ACCT, Changed

Message

```
<timestamp>
INFO SEC-ACCT, 4, <message> Changed account <user name>
```

Probable Cause

The specified account has changed.

Recommended Action

No action is required.

Severity

INFO

SEC-ACCT, Deleted

Message

```
<timestamp>
INFO SEC-ACCT, 4, <message> Deleted account <user name>
```

Probable Cause

An existing account was deleted.

Recommended Action

No action is required.

Severity

INFO

SEC-ACCT, Recovered

Message

```
<timestamp>
INFO SEC-ACCT, 4, <message> Recovered <number of> accounts
```

Probable Cause

The specified number of accounts were recovered from backup.

Recommended Action

No action is required.

Severity

INFO

SEC-INITERR

Message

```
<timestamp>

ERROR SEC-INITERR, 2, Initialization failed: Switch is not security
capable. Disabling Security mode.
```

Probable Cause

The `secmodeenable` command failed because the switch does not support secure mode.

Recommended Action

Check that all conditions required for secure mode are installed on the switch. Correct any missing requirements, such as a missing zoning license, RCS capability, or the PID mode on the switch. Refer to the *HP StorageWorks Secure Fabric OS Version 1.0 User Guide* for more information on secure mode requirements.

Severity

ERROR

SEC-PIDCHGERR, PID Change failed: Change Area failed

Message

```
<timestamp>

ERROR SEC-PIDCHGERR, 2, PID Change failed: Change Area failed. <defined
status> <active status>
```

Probable Cause

Either the defined or active policy could not be updated. If the policy database is very large, it might not be able to change the area because the new policy database exceeds the maximum size. This message can also be caused when the switch is short of memory. The status values can be `defined`, `active`, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

Reduce the size of the policy database.

Severity

ERROR

SEC-PIDCHGERR, PID Change failed: Size check failed

Message

```
<timestamp>

ERROR SEC-PIDCHGERR, 2, PID Change failed: Size check failed. <defined
status> <active status>
```

Probable Cause

Either the new defined or new active policy was too large after modifying the area ID. The status values can be `defined`, `active`, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

Reduce the size of the specified policy database.

Severity

ERROR

SEC-PIDCHGERR, Change failed: Can't get sec_db

Message

```
<timestamp>

ERROR SEC-PIDCHGERR, 2, Change failed: Switch is busy. Operation failed.
```

Probable Cause

The switch security daemon is busy. The status values can be `defined`, `active`, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

For the first reject, wait a few minutes and then resubmit the transaction. Fabric-wide commands might take a few minutes to propagate throughout the fabric. Make sure to leave enough time so your commands do not overlap in the fabric.

Severity

ERROR

SEC-PIDCHGINFO

Message

```
<timestamp>
INFO SEC-PIDCHGINFO, 4, PID Change: Success
```

Probable Cause

The PID format of the switch was changed either to extended-edge PID or from extended-edge PID. If DCC policies existed, all area ID values either increased or decreased by 16. The values wrap around after a port value of 128. If a DCC policy contains an area of 127 before changing to extended edge PID, the new area is 15 because of the wraparound.

Recommended Action

No action is required.

Severity

INFO

SEC-RSENDFAIL

Message

```
<timestamp>
ERROR SEC-RSENDFAIL, 2, RCS process fails: %s
```

Probable Cause

The Reliable Commit Service (RCS) process failed to complete. RCS is a reliable mechanism to transfer data from one switch to the other switches within the fabric. This mechanism guarantees that either all switches commit to the new database or none of them update to the new database. This process can fail if one switch in the fabric is busy or in an error state that can not accept the database.

Recommended Action

RCS is used when the security database is changed by a command issued by security (for example, `secpolicysave`, `secpolicyactivate`, and `secversionreset`). If the switch is busy, the command might fail the first time; retry the command.

If the command fails consistently, copy the message, collect switch information using the `supportshow` command, and contact your switch service provider.

Severity

ERROR

SEC-SECCHANGE

Message

```
<timestamp>
INFO SEC-SECCHANGE, 4, text message
```

Probable Cause

A security admin event occurred. This message is for information purposes only, but you should verify that the event was planned. The text messages for individual events are:

- `secmodeenable`: Secure mode was enabled.
- `secmodedisable`: Secure mode was disabled.
- `secpolicyactivate`: A, B, C policies were changed. (A, B, C are names for changed policies.)
- `secversionreset`: Secure fabric version stamp was reset.
- `secfcsfailover`: The primary FCS has failed over to a new switch.
- All password changes: A, B, C account passwords were changed. (A, B, C are account names for which passwords are changed.)
- `configdownload`: A configdownload was executed that changed the security policy database.
- `secpolicysave`: A change to the security policy database was saved.
- SNMP community string change: The admin has made a change to the SNMP community strings.

Recommended Action

Verify that the security event was planned:

- If the security event was planned, no action is required.
- If the security event was not planned, investigate the action and verify that it was authorized.

Severity

INFO

SEC-SECDBFAIL

Message

```
<timestamp>
WARNING SEC-SECDBFAIL, 3, <text message>
```

Probable Cause

The receiving switch failed to validate the security database sent from the primary FCS switch. This message usually indicates that the data package is corrupted, the timestamp on the package is out of range as a result of replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action

Issue the `secfabricshow` command to verify that the fabric is still consistent. All the switches should be in the READY state. If a switch is in the ERROR state, the database might not be correctly updated for that specific switch. The error might also be a result of an internal corruption or a hacker attack to the secure fabric.

Severity

WARNING

SEC-SECDLFAIL

Message

```
<timestamp>
WARNING SEC-SECDLFAIL, 3, Fail to download security data to domain <domain
number> after <number of retries> retries
```

Probable Cause

The specified domain number failed to download security data after the specified number of attempts. The primary switch segments the failed switch after 30 tries. The failed switch might have had some internal error and failed to accept the database download.

Recommended Action

This might be an internal resource issue; rejoin the switch to the fabric and the security data download retries.

If the command fails consistently, copy the message, collect switch information using the `supportshow` command, and contact your switch service provider.

Severity

WARNING

SEC-SEC_INFO

Message

```
<timestamp>
INFO SEC-SEC_INFO, 4, <text_message>
```

Probable Cause

Indicates one of the following:

- Low memory
- Queue full
- Failure to set password
- Failure to set SNMP string
- Failure to sign message
- Primary FCS downloads security database
- Nonprimary FCS switch receives security database download

Recommended Action

This is usually a transient problem. Retry the command that caused the message.

Severity

INFO

SEC-SECINFORM

Message

```
<timestamp>
INFO SEC-SECINFORM, 4, Primary FCS receives data request from domain
<domain number>
```

Probable Cause

The primary FCS received a data request from the specified domain. For example, if the switch fails to update the database or is attacked (data injection), a message is generated to the primary FCS to try to correct and resync with the rest of the switches in the fabric.

Recommended Action

Check the fabric status using `secfabricshow` to verify that the fabric is not being attacked by unauthorized users.

Severity

INFO

SEC-SEC_STATS

Message

```
<timestamp>
WARNING SEC-SEC_STATS, 3, Security statistics error:
```

Probable Cause

A statistics-related command for security (`secstatsshow` or `secstatsreset`) was logged. The counter is updated automatically when a security violation occurs. This message might also occur if the updating counter fails.

Recommended Action

If the message is the result of a user command, retry the `statistic` command.

Severity

WARNING

SEC-SECVIOL_API

Message

```
<timestamp>
INFO SEC-SECVIOL_API, 4, Security violation: Unauthorized host with IP
address <IP address> tries to establish API connection.
```

Probable Cause

An API security violation was reported. The specified unauthorized host attempted to establish an API connection.

Recommended Action

Check to see if the host IP address specified in the message can be used to manage the fabric through an API connection. If so, add the host IP address to the API policy of the fabric. If not, this is an unauthorized access; take the appropriate action as per your enterprise security policy.

Severity

INFO

SEC-SECVIOL_HTTP

Message

```
<timestamp>

INFO SEC-SECVIOL_HTTP, 4, Security violation: Unauthorized host with IP
address <IP address> tries to establish HTTP connection.
```

Probable Cause

An HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

Recommended Action

Check to see if the host IP address specified in the message can be used to manage the fabric through an HTTP connection. If so, add the host IP address to the HTTP policy of the fabric. If not, this is an unauthorized access; take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_TELNET

Message

```
<timestamp>

INFO SEC-SECVIOL_TELNET, 4, Security violation: Unauthorized host with IP
address <IP address> tries to establish TELNET session.
```

Probable Cause

A telnet security violation was reported. The specified unauthorized host attempted to establish a telnet connection.

Recommended Action

Check to see if the host IP address specified in the message can be used to manage the fabric through a telnet connection. If so, add the host IP address to the telnet policy of the fabric. If not, this is an unauthorized access; take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_DCC

Message

```
<timestamp>
INFO SEC-SECVIOL_DCC, 4, Security violation: Unauthorized device <device
node name> tries to flogin to port <port number> of switch <port node
name>.
```

Probable Cause

A DCC security violation was reported. The specified device attempted to perform a FLOGI operation to an unauthorized port. The DCC policy correlates specific devices to specific port locations. If the device changes connected port, the device is not allowed to perform FLOGI.

Recommended Action

Check the DCC policy and verify that the specified device is allowed in the fabric and is included in the DCC policy. If the specified device is not included in the policy, add it to the policy. If the device is not allowed, this is a valid violation message and an unauthorized entity is trying to gain access to your fabric; take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_LOGIN

Message

```
<timestamp>
INFO SEC-SECVIOL_LOGIN, 4, Security violation: Login failure attempt via
<connection method>.  Peer IP: <IP address>
```

Probable Cause

A login security violation was reported. An incorrect password was used while trying to log in through a console, telnet, HTTP, or API connection; the login failed.

Recommended Action

Use the correct password.

Severity

INFO

SEC-SECVIOL_MSaccess

Message

```
<timestamp>

INFO SEC-SECVIOL_MSaccess, 4, Security violation: Unauthorized access from
MS device node name <device node name>, device port name <device port
name>.
```

Probable Cause

A management server security violation was reported. The specified unauthorized management server (MS) device attempted to establish a connection.

Recommended Action

Check the management server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy.

If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_MSfwrd

Message

```
<timestamp>

INFO SEC-SECVIOL_MSfwrd, 4, Security violation: MS command is forwarded
from non primary FCS switch.
```

Probable Cause

An MS forward security violation was reported. A management server command was forwarded from a nonprimary FCS switch.

Recommended Action

Check the management server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in MS policy.

If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_MSop

Message

```
<timestamp>

INFO SEC-SECVIOL_MSop, 4, Security violation: MS device <device wwn>
operates on non primary FCS switch.
```

Probable Cause

An MS operation security violation was reported. A management server device is operating on a nonprimary FCS switch.

Recommended Action

Check the management server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy.

If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_RSNMP

Message

```
<timestamp>

INFO SEC-SECVIOL_RSNMP, 4, Security violation: Unauthorized host with IP
address <IP address> tries to do SNMP read operation.
```

Probable Cause

An SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP operation (RSNMP).

Recommended Action

Check RSNMP policy to verify that hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy. If the host is allowed access to the fabric but is not included in the RSNMP policy, add the host to the policy.

If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_SCC

Message

```
<timestamp>
INFO SEC-SECVIOL_SCC, 4, Security violation: Unauthorized switch <switch
wwn> tries to join secure fabric.
```

Probable Cause

An SCC security violation was reported. The specified unauthorized switch attempts to join the secure fabric.

Recommended Action

Check the Security Connection Control policy (SCC policy specifies the WWNs of switches allowed in the fabric) to verify which switches are allowed in the fabric. If the switch is allowed in the fabric but not included in the SCC policy, add the switch to the policy.

If the switch is not allowed in the fabric, this is a valid violation message and an unauthorized entity is trying to access the fabric. Take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_SERIAL

Message

```
<timestamp>
INFO SEC-SECVIOL_SERIAL, <text message>
```

Probable Cause

A serial connection policy security violation was reported. An attempt was made to access the serial console when it is disabled.

Recommended Action

Determine whether an unauthorized access attempt is being made on the console. Take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-SECVIOL_WSNMP

Message

```
<timestamp>

INFO SEC-SECVIOL_WSNMP, 4, Security violation: Unauthorized host with IP
address <IP address> tries to do SNMP write operation.
```

Probable Cause

An SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation (WSNMP).

Recommended Action

Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy.

If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action as defined by your enterprise security policy.

Severity

INFO

Extended fabric user guide

5

This chapter contains updates to the *HP StorageWorks Extended Fabric Version 3.1.x/4.1.x User Guide*, part number AA-RTSDC-TE.

On page 26, under the heading "VC Translation Mode," replace the following text:

VC_Translation_Link_Init

Specify `1` to activate long distance link initialization sequence. This mode is used to initiate long distance connections. When configuring a long distance connection, the first port configured does not require this mode. When configuring the second port of a connection, use this mode to initiate communication between the ports.

With this text:

Specify `1` to activate the long-distance link initialization sequence for all ports, including the first port configured.

Note: For information on trunking over extended fabrics in Fabric OS v3.2.x, see the trunking chapter of this document.

Fabric OS procedures user guide

6

This chapter contains updates to the *HP StorageWorks Fabric OS Procedures Version 3.1.x/4.1.x User Guide*, part number AA-RS23C-TE.

On page 47, in the section "Domain IDs," add the following information:

Domain IDs are assigned dynamically when a switch is enabled. The domain ID can be set manually, however, to control the number or to resolve a domain ID conflict when merging fabrics.

Note: If a switch already has a domain ID and that domain ID conflicts with a switch already in the fabric, the conflict is resolved. If a switch with a conflicting domain ID is hot-plugged or connected to a fabric while it is enabled, it segments with a `domain overlap` message.

Add the following new chapter after Chapter 2:

Configuring Standard Security Features

This chapter provides information and procedures for standard Fabric OS security features.

Standard Fabric OS security features include account and password management.

Additional security is available when secure mode is enabled. For information about licensed security features available in Secure Fabric OS, refer to the *HP StorageWorks Secure Fabric OS Version 1.0 User Guide*.

Ensuring Network Security

To ensure security, Fabric OS supports secure shell (SSH) encrypted sessions. SSH encrypts all messages, including the client's transmission of password during login. The SSH package contains a daemon (sshd), which runs on the switch. The daemon supports a wide variety of encryption algorithms, such as Blowfish-CBC and AES.

Note: To maintain a secure network, avoid using telnet or any other unprotected application when you are working on the switch. For example, if you use telnet to connect to a machine and then start an SSH or secure telnet session from that machine to the switch, the communication to the switch is in clear text, and therefore is not secure.

The FTP protocol is also not secure. When you use FTP to copy files to or from the switch, the contents are in clear text. This includes the remote FTP server's login and password. This limitation affects the following commands: `savecore`, `configupload`, `configdownload`, and `firmwaredownload`.

Commands that require a secure login channel must be issued from an original SSH session. If you start an SSH session and subsequently use the `login` command to start a nested SSH session, commands that require a secure channel are rejected.

Fabric OS v3.2.x and later supports SSH protocol v2.0 (ssh2). For more information on SSH, see the SSH IETF web site: http://www.ietf.org/ids.by.wg/secsh.html .

Fabric OS v3.2.x comes with the SSH server preinstalled; however, you must select and install the SSH client. For information on installing and configuring the F-Secure SSH client, see the web site: http://www.f-secure.com .

Accessing Switches and Fabrics

You can disable HTTP, SNMP, and RPC access to Fabric OS switches using the `configure` command. Disabling these access points helps make a fabric more secure.

Following is sample output from the `configure` command:

```
switch:admin> configure
Configure...

Fabric parameters (yes, y, no, n): [no]
Virtual Channel parameters (yes, y, no, n): [no]
Zoning Operation parameters (yes, y, no, n): [no]
RSCN Transmission Mode (yes, y, no, n): [no]
Arbitrated Loop parameters (yes, y, no, n): [no]
System services (yes, y, no, n): [no]

rstatd (on, off): [off]
rusersd (on, off): [off]
rapid (on, off): [on]
thad (on, off): [on]
Disable RLS probing (on, off): [on]
Portlog events enable (yes, y, no, n): [no]
Configure Application Attributes:

http:
HTTP Enabled (yes, y, no, n): [yes]
snmp:
SNMP Enabled (yes, y, no, n): [yes]
rpc:
RPCd Enabled (yes, y, no, n): [yes]
switch:admin> version
```

Table 12 lists the defaults for accessing hosts, devices, switches, and zones.

Table 12: Access Defaults

Area	Default
Hosts	Any host can access the fabric by SNMP.
	Any host can use telnet to any switch in the fabric.
	Any host can establish an HTTP connection to any switch in the fabric.
	Any host can establish an API connection to any switch in the fabric.
Devices	All device ports can access SES.
	All devices can access the management server.
	Any device can connect to any FC port in the fabric.
Switches	Any switch can join the fabric.
	All switches in the fabric can be accessed through the serial port.
Zones	Node WWNs can be used for WWN-based zoning.

Creating and Maintaining User-Defined Accounts

In addition to the default administrative and user accounts, Fabric OS supports up to 15 user-defined accounts in each logical switch (domain). These accounts expand your ability to track account access and audit administrative activities.

User-defined accounts can be specified as either admin or user level. Admin-level accounts allow up to two simultaneous login sessions. User-level accounts allow up to four simultaneous login sessions. The total number of simultaneous login sessions allowed per logical switch is 15.

You can change passwords on user-defined accounts as described in “Changing an Account Password.”

If the track changes feature is enabled, the system keeps track of account names and login attempts.

For large enterprises, Fabric OS also supports RADIUS services, as described in “Setting Up RADIUS AAA Service.”

The following procedures are for operations you can perform on user-defined accounts.

Note: If you are operating in secure mode, you can perform these operations only on the primary FCS switch.

To display account information:

Note: Accounts with the admin role can display information about all accounts on the logical switch. Accounts with the user role can display information only about themselves.

1. Connect to the switch and log in as admin.
2. Issue one of the following commands:

- `userConfig “--show -a”`
  Shows all account information for a logical switch.
- `userConfig “--show -b”`
  Shows all backup account information for a logical switch. HP recommends that you make a backup copy of the configuration file in case the configuration is lost or unintentional changes are made. Keep individual backup files for all switches in the fabric.
- `userConfig “--show name”`
  Shows account information for the specified account name.

To create a user-defined account:

Note: Accounts with the admin role can create accounts. Accounts with the user role cannot.

1. Connect to the switch and log in as admin.
2. Issue the following command:

```
userConfig ”--add name -r rolename [-d description]“
```

where:

name Specifies the account name, which must begin with an alphabetic character. The name can contain up to 40 characters. It is case-sensitive and can contain alphabetic and numeric characters, the dot (.), and the underscore (_). It must be different from all other account names on the logical switch.

-r *rolename* Specifies the role: either admin or user in nonsecure mode; admin, user, or nonfcsadmin in secure mode.

-d *description* Is an option that adds a description to the account. The description field can contain up to 40 printable ASCII characters. The following characters are not allowed: asterisk (*), quotation mark (“), exclamation point (!), semicolon (;), and colon (:).

3. In response to the prompt, enter a password for the account.

   Passwords can be from 8 to 40 characters long. They are case-sensitive, and they are not displayed when you enter them on the command line.

To delete a user-defined account:

Note: Accounts with the admin role can delete user-defined accounts on the logical switch. Accounts with the user role cannot.

1. Connect to the switch and log in as admin.

2. Issue the following command:

   ```
   userConfig ”--delete name“
   ```

   where *name* Specifies the account name. You cannot delete the default accounts. An account cannot delete itself. All active CLI sessions for the deleted account are logged out.

3. At the prompt for confirmation, enter `y`**.**

To change account parameters:

Note: Accounts with the admin role can change information for all accounts with lower permission on the logical switch. Accounts with the user role cannot.

---

1. Connect to the switch and log in as admin.
2. Enter the following command:

   ```
   userConfig ”--change username [-r rolename] [-d description] [-e yes | no]“
   ```

where:

`username`

Changes the account attribute for username. The account must already exist on the switch.

`-r` *`rolename`*

Is an option that changes the role: either admin or user in nonsecure mode; admin, user, or nonfcsadmin in secure mode.

An account cannot change its own role.

You can change the role name only of a user-defined account with a lower level of authorization.

`-d` *`description`*

Is an optional account description. The description field can contain up to 40 printable ASCII characters. The following characters are not allowed: asterisk (*), quotation mark (“), exclamation point (!), semicolon (;), and colon (:).

You can change the description only of a user-defined account with a lower level of authorization.

`-e`

Is an option; enter `yes` to enable the account or `no` to disable it. If you disable an account, all active CLI sessions for that account are logged out. You can enable or disable user-defined or default accounts.

To recover user-defined accounts:

If a backup account exists (in secure mode), you can recover it with the following command:

```
userConfig ”--recover“
```

The following conditions apply to recovering user accounts:

- Only accounts with admin or higher roles can recover accounts.
- The attributes in the backup database replace the attributes in the current account database.
- An event is stored in the system message log, indicating that accounts were recovered.

Changing an Account Password

At each level of account access, you can change passwords for that account and accounts that have lesser privileges.

If you log in to a user account, you can change only that account's password.

If you log in to an admin account, you can change admin and user passwords. You must provide the old password when the account being changed has the same or higher privileges than the current login account. For example, when logged in as admin, you need admin passwords to change passwords for admin accounts (except when you change the default user account password at login), but you do not need user passwords to change passwords for user accounts.

A new password must have at least one character different from the old password. The following rules also apply to passwords:

- You cannot change passwords using SNMP.
- Password prompting is disabled when security mode is enabled.
- Starting with Fabric OS v3.2.x, you cannot change default account names.

To change the password for the current login account:

1. Connect to the switch and log in as either admin or user.
2. Enter the following command:

   ```
   passwd
   ```
3. Enter the requested information at the prompts.

To change the password for a different account:

1. Connect to the switch and log in as admin.
2. Enter the following command:

   ```
   passwd name
   ```

where *name*	Specifies the account name.

3. Enter the requested information at the prompts.

   If the named account has lesser privileges than the current account, the old password is not required. If the named account has equal or higher privileges than the current account, you are prompted to enter the old password.

Setting Up RADIUS AAA Service

Fabric OS supports RADIUS authentication, authorization, and accounting service (AAA). When configured for RADIUS, the switch becomes a RADIUS client. In this configuration, authentication records are stored in the RADIUS host server database. Login and logout account name, assigned role, and time-accounting records are also stored on the RADIUS server.

Set up RADIUS service through a secure connection such as SSH.

By default, RADIUS service is disabled, so AAA services default to the switch local database.

To enable RADIUS service, access the CLI through an SSH connection so that the shared secret is protected. Multiple login sessions can configure simultaneously, and the last session to apply a change leaves its configuration in effect. After a configuration is applied, it persists after a reboot or an HA failover.

The configuration is chassis-based, so it applies to all logical switches (domains) on the switch and replicates itself on a standby CP card, if one is present. It is saved in a firmware upload, so it can be applied to other switches in a firmware download. Configure at least two RADIUS servers so that if one fails, the other assumes service. You can set the configuration with both RADIUS service and local authentication enabled so that if all RADIUS servers do not respond (because of power failure or network problems), the switch uses local authentication.

Considerations for RADIUS Use

Consider the following effects of the use of RADIUS service on other Fabric OS features:

- Passwords
  - When RADIUS service is enabled, all account passwords must be managed on the RADIUS server. The Fabric OS mechanisms for changing switch passwords remain functional; however, such changes affect only the involved switches locally. They do not propagate to the RADIUS server, nor do they affect any account on the RADIUS server.
  - When RADIUS is set up for a fabric that contains a mix of switches running v4.4.0, v3.2.x, or earlier, the way a switch authenticates users depends on whether a RADIUS server is set up for that switch. For a switch with RADIUS support and configuration, authentication bypasses the local password database. For a switch without RADIUS support or configuration, authentication uses switch local account names and passwords.
- Secure Fabric OS. In secure mode, the following items apply:
  - Account passwords are distributed among all switches in the same fabric. An account that resides on several switches has the same password on all of them. This model applies with RADIUS integration; such a distribution affects only the switch local password database.
  - There are separate admin and nonfcsadmin roles in secure mode. A nonfcsadmin account on a RADIUS server cannot access FCS switches, even if the account is properly authenticated.
  - If a nonfcsadmin account on a RADIUS server logs in to a switch in nonsecure mode, the switch treats the role like the admin role and grants the access.
  - The secure Fabric OS telnet policy does not affect the operation of the RADIUS protocol.
- Advanced Web Tools. The following items apply:
  - Advanced Web Tools client and server keep an open session after a user is authenticated. A password change on a switch invalidates an open session and requires the user to log in again. When integrated with RADIUS, a switch password change on the RADIUS server does not invalidate an existing open session. However, a password change on the local switch does invalidate an existing open session.
  - If you cannot log in because of a RADIUS server connection problem, Advanced Web Tools displays a message indicating server outage.

- API. The following items apply:
  - When an older version of the API host library authenticates against a switch with RADIUS support, the host performs the login. However, the old host library does not recognize the role returned from the switch, which can result in the host displaying an incorrect read or write attribute for an account. The switch library performs the permission check again for individual API function calls.
  - API provides functions for RADIUS configuration that share the behavior of the `aaaconfig` CLI command.
- Advanced Web Tools *and* API. The following items apply to both of these features:
  - Users can log in using account names and passwords configured on the RADIUS server, and gain access with the switch roles defined on the RADIUS server.
  - Users can log in through API using account names and passwords configured on the RADIUS server, and gain access with the switch roles defined on the RADIUS server.
  - When a proxy switch is used, the switch-side component performs authentication on the proxy switch, rather than on the destination switch. Therefore, to use RADIUS in this environment, you must configure on the proxy switch.

Accounting Support

The RADIUS service supports accounting request and response packets so that accounting records can be centralized on the RADIUS server. The login account name, assigned role, and password are stored on the RADIUS server for each user.

Setting Up the RADIUS Server

You must know the switch IP address or name to connect to switches. Use the `ipaddrshow` command to display a switch IP address.

User accounts should be set up by their true network-wide identity, rather than by the account names created on a Fabric OS switch. Along with each account name, the administrator should assign appropriate switch access roles. To manage a nonsecure fabric, these roles can be user or admin. To manage a secure fabric, these roles can be user, admin, or nonfcsadmin.

When they log in to a switch configured with RADIUS, users enter their assigned RADIUS account names and passwords at the prompt. After the RADIUS server authenticates a user, it responds with the assigned switch role in an HP Vendor-Specific Attribute (VSA) as defined in the RFC. An authentication-accept response without such VSA role assignment grants the user role.

The following sections explain how to configure a RADIUS server to support HP clients under different operating systems.

Windows 2000

Use these procedures to add a client to the RADIUS server and create remote access policies for Fabric OS user and admin roles.

To add a RADIUS client:

1. From the Windows **Start** menu, select **Programs > Administrative Tools:Internet Authentication Service**.
2. In the Internet Authentication Service window, right-click the **RADIUS Clients** folder and select **New RADIUS Client**.

3. In the New RADIUS Client window:
   - In the Friendly name space, enter a name for the switch that allows you to identify it easily.
   - In the Client Address (IP or DNS) space, enter the IP address of the switch.
4. Click **Next**.
5. In the next window, enter and confirm the shared secret in the spaces provided. Make sure the shared secret matches that configured on the switch (as described in "Adding a RADIUS Server.")
6. Click **Finish**.

The new client friendly name appears in the list of clients. To change the shared secret, right-click the client, select **Properties**, and change the secret in the properties window.

To create user and admin remote access policies:

1. From the Windows **Start** menu, select **Programs > Administrative Tools:Internet Authentication Service** to bring up the Internet Authentication Service window.
2. If you do not already have Windows groups set up, use standard Windows procedures to set up a Windows group of login names assigned to the user role and another Windows group of login names assigned to the admin role.
3. Right-click the **Remote Access Policies** icon folder and select **New Remote Access Policy**.
4. In the New Remote Access Policy Wizard window, click **Next**.
5. In the Set Up a Custom Policy window:
   - Select the **Custom policy** radio button.
   - Enter a policy name for the user role (for example, `HP User`) in the space provided.
   - Click **Next**.
6. In the Select Attribute window, select **Windows-Groups** and click **Add**.
7. In the Select Groups window:
   - Enter the name of the Windows group that contains login names assigned to the user role.
   - Click **Check Names**.

     When the system finds the Windows group, it underlines the name.
8. Click **OK**.
9. In the Group window, check that the Windows group is listed and then click **OK**.
10. In the Policy Conditions window, check that the policy name is listed (for example, `HP User`) and then click **Next**.
11. In the Permissions window, select the **Grant remote access permission** radio button and then click **Next**.
12. In the Profile window, click **Edit Profile**.
13. In the Edit Dial-in Profile window, select the **Authentication** tab.

14. In the **Authentication** tab:
    - Uncheck the following check boxes:
        - Microsoft® Encryption (MSCHAPv2)
        - Microsoft Encryption (MSCHAP)
    - Check the following check boxes:
        - Encrypted Authentication (CHAP)
        - Unencrypted Authentication (PAP, SPAP)
15. Select the **Advanced** tab.
16. In the **Advanced** tab, click **Add**.
17. In the Add Attributes window, select **Vendor-specific** and click **Add**.
18. In the **Multivalued Attribute Information** window, click **Add**.
19. In the **Vendor-Specific Attribute Information** window:
    - Select the **Enter Vendor Code** radio button and enter `1588` in the space provided.
    - Select the **Yes. It conforms.** radio button.
    - Click **Configure Attribute**.
20. In the Configure VSA (RFC Compliant) window, enter the following information in the spaces provided:
    - Vendor-Assigned Attribute Number: `1`
    - Attribute Format: `string`
    - Attribute Value: `user`
21. Click **OK**.
22. Click **OK** or **Close** in each window until you reach the New Remote Access Policy Wizard.
23. Click **Next**.
24. Click **Finish**.
25. Repeat the procedure to set the admin remote access policy, with the following differences:
    - In step 5, enter a policy name for the admin role (for example, `HP Admin`) in the space provided.
    - In step 7, enter the name of the Windows group that contains login names assigned to the admin role.
    - In step 20, enter `admin` in the Attribute Value space.

Linux

Use the following procedure on a Linux FreeRADIUS server to:

- Set up a vendor dictionary file and include it in the system dictionary file.
- Identify a switch as a RADIUS client.
- Set up user accounts and roles.

- Test the configuration.

1. Log in to the server and change directory to the RADIUS configuration file directory. Typically, this directory is located at `/usr/local/etc/raddb`.
2. Use a text editor to create a vendor dictionary file called `dictionary.hp` and enter the following lines into the file:

```
#
# dictionary.hp
#
VENDOR     HP            1588
#
# attributes
#
ATTRIBUTE HP-Auth-Role  1       string      HP
```

3. Save `dictionary.hp`.
4. Open the `dictionary` file in a text editor and add this line:

```
$INCLUDE dictionary.hp
```

5. Save the `dictionary` file.
6. Open the `client.config` file in a text editor and add the switches that are to be configured as RADIUS clients. For example, to configure the switch at IP address 10.32.170.59 as a client:

```
client 10.32.170.59
   secret      = Secret
   shortname   = Testing Switch
   nastype     = other
```

   In this example, the switch name is `Testing Switch` and its shared secret is `Secret`. Make sure that the shared secret matches that configured on the switch (see "Adding a RADIUS Server").

7. Save `client.config`.
8. Open the `user` file in a text editor and add user names and roles for users who will be accessing the switch. For example, to set up an account called `JohnDoe` with the admin role:

```
JohnDoe Auth-Type := Local, User-Password == "johnPassword"
HP-Auth-Role = "admin"
```

9. Save the `user` file.
10. Enter the following command to start the RADIUS server:

    `/usr/local/sbin/radiusd`

11. Log in to a client switch and issue the `aaaconfig` command to configure it as a client and enable RADIUS service, as described in "Adding a RADIUS Server" and "Enabling and Disabling RADIUS Service."
12. Log out.

When you log in to the switch again, RADIUS service is in force.

Setting Up the Switch

The following procedures show how to use the `aaaconfig` command to set up a single switch for RADIUS service. You can also set up multiple switches simultaneously with the HP Fabric Manager optional software tool.

To display the current RADIUS configuration, issue the command:

```
aaaConfig ”--show“
```

If a configuration exists, its parameters are displayed. If RADIUS service is not configured, only the parameter heading line is displayed. Parameters are:

`Position`	The order in which servers are contacted to provide service
`Server`	The server names or IP addresses
`Port`	The server ports
`Secret`	The shared secrets
`Timeouts`	The length of time servers have to respond before the next server is contacted
`Authentication`	The type of authentication being used on servers

To add a RADIUS server to the configuration, issue the command:

```
aaaConfig ”--add server [-p port] [-s secret] [-t timeout] [-a]–“
```

where:

`server`	Is a server name or IP address. Avoid duplicating server listings (that is, listing the same server once by name and again by IP address). Up to five servers can be added to the configuration.
`-p` *`port`*	Is an option; enter a server port. The default is port 1812.
`-s` *`secret`*	Is an option; enter a shared secret. The default is `sharedsecret`. Secrets can contain 8 to 40 alphanumeric characters.
`-t` *`timeout`*	Is an option; enter the length of time (in seconds) the server has to respond before the next server is contacted. The default is 3 seconds. Timeout values can range from 1 to 30 seconds.
`-a`	Is an option; specify that the PAP protocol be used instead of the CHAP protocol for packets traveling between the switch and the server.

Enabling and Disabling RADIUS Service:

At least one RADIUS server must be configured before you can enable RADIUS service.

To enable or disable RADIUS service, issue the command:

```
aaaConfig ”--radius on | off“
```

Specifying `on` enables the service; specifying `off` disables it.

If no RADIUS configuration exists, turning it on triggers an error message. When the command succeeds, an event is sent to the event log, indicating that the configuration is enabled or disabled.

To delete a RADIUS server from the configuration:

1. Issue the following command:

   ```
   aaaConfig ”--remove server | all“
   ```

   where:

   server Is a server listed either by name or IP address. Enter either the name or IP address of the server to be removed.

   all Is a keyword that removes all servers. If RADIUS service is enabled, this removes all but the server in the first position. If RADIUS service is disabled, all servers are removed.

2. At the prompt, enter y to complete the command.

When the command succeeds, an event is sent to the event log, indicating that the server is removed.

To change the parameters of a RADIUS server that is already configured, issue the following command:

```
aaaConfig ”--change server [-p port] [-s secret] [-t timeout]
[-a pap | chap]“
```

where:

server Is a server listed either by name or IP address. Enter either the name or IP address of the server to be changed.

-p *port* Is an option; enter a server port.

-s *secret* Is an option; enter a shared secret.

-t *timeout* Is an option; enter the length of time (in seconds) the server has to respond before the next server is contacted.

-a pap | chap Is an option; specify that the PAP protocol be used instead of the CHAP protocol for packets traveling between the switch and the server.

To change the order in which RADIUS servers are contacted for service, issue the following command:

```
aaaConfig ”--move server to_position“
```

where:

server Is a server listed either by name or IP address. Enter either the name or IP address of the server whose position order is to be changed.

to_position Is the number of the position to which the server is to be moved.

When the command succeeds, it triggers an event log, indicating that a server configuration is changed.

Enabling and Disabling Local Authentication:

It is useful to enable local authentication so that the switch can take over authentication locally if the RADIUS servers fail to respond because of power outage or network problems. To enable or disable local authentication, issue the following command:

```
aaaConfig ”--switchdb on | off“
```

Specifying `on` enables local authentication; specifying `off` disables it.

When local authentication is enabled and RADIUS servers fail to respond, you can log in to the default switch accounts (admin and user) or any user-defined account. You must know the passwords of these accounts.

RADIUS authentication must be enabled when local database authentication is turned off; otherwise, an error is returned. The local database cannot be turned off unless RADIUS has already been configured.

Because local database authentication might be automatically disabled or enabled when enabling or disabling RADIUS authentication, set the local database authentication explicitly to enabled or disabled after setting the desired RADIUS authentication configuration.

When the command succeeds, it triggers an event log, indicating that local database authentication is disabled or enabled.

Configuring for SNMP

You can configure SNMP agents. Fabric OS v3.2.x supports SNMPv1.

The configuration process involves configuring the SNMP agents, MIBs, and traps. The following commands are used in the process:

- Use the `configure` command to enable and disable for SNMPv1.
- Use the following commands to configure for SNMPv1:
  - Use the `agtCfgShow`, `agtCfgSet`, and `agtCfgDefault` commands to configure the SNMPv1 agent.
  - Use the `snmpmibcapset` command to turn on and off certain MIBs and traps.

For details about configuring MIBs, see Chapter 8, “Fabric OS reference guide.”

If you use both SW-MIB and FA-MIB, you might receive duplicate information. You can disable the FA-MIB, but the SW-MIB cannot be disabled.

If you enable the SW-EXTTRAP option, the Software Serial Number (swSsn) is included as a part of HP SW traps. It is also used in conjunction with the legacy StorgeWorks SAN Switch Integrated/64 to provide detailed group information for a particular trap.

For information on the specific commands used in these procedures, refer to online help or to the *HP StorageWorks Fabric OS 3.1.x/4.1.x Reference Guide.*

Configuring for SNMPv1

Use the following procedures to configure the SNMPv1 agent and traps. To display SNMP agent configuration information:

Issue the `agtCfgShow` command, as in the following example:

```
switch:admin> agtcfgshow
Current SNMP Agent Configuration
         Customizable MIB-II system variables:
                 sysDescr = FC Switch
              sysLocation = End User Premise
               sysContact = Field Support.
                authTraps = 1 (ON)

     SNMPv1 community and trap recipient configuration:
       Community 1: Secret C0de (rw)
         Trap recipient: 192.168.1.51
         Trap recipient Severity level: 4
       Community 2: OrigEquipMfr (rw)
         Trap recipient: 192.168.1.26
         Trap recipient Severity level: 0
       Community 3: private (rw)
         No trap recipient configured yet
       Community 4: public (ro)
         No trap recipient configured yet
       Community 5: common (ro)
         No trap recipient configured yet
       Community 6: FibreChannel (ro)
         No trap recipient configured yet

     SNMP access list configuration:
     Entry 0:  Access host subnet area 192.168.64.0 (rw)]
     Entry 1:  No access host configured yet
     Entry 2:  No access host configured yet
     Entry 3:  No access host configured yet
     Entry 4:  No access host configured yet
     Entry 5:  No access host configured yet
```

To modify the SNMP configuration values, issue the `agtCfgSet` command, as in the following example:

```
switch:admin> agtcfgset

     Customizing MIB-II system variables ...

     At each prompt, do one of the followings:
       o <Return> to accept current value,
       o enter the appropriate new value,
       o <Control-D> to skip the rest of configuration, or
       o <Control-C> to cancel any change.

     To correct any input mistake:
     <Backspace> erases the previous character,
     <Control-U> erases the whole line,
     sysDescr: [FC Switch]
     sysLocation: [End User Premise]
     sysContact: [Field Support.]
     authTrapsEnabled (true, t, false, f): [true]

     SNMP community and trap recipient configuration:
     Community (rw): [Secret C0de]
     Trap Recipient's IP address in dot notation: [192.168.1.51]
     Trap recipient Severity level : (0..5) [0] 3
     Community (rw): [OrigEquipMfr]
     Trap Recipient's IP address in dot notation: [192.168.1.26]
     Trap recipient Severity level : (0..5) [0]
     Community (rw): [private]
     Trap Recipient's IP address in dot notation: [0.0.0.0] 192.168.64.88
     Trap recipient Severity level : (0..5) [0] 1
     Community (ro): [public]
     Trap Recipient's IP address in dot notation: [0.0.0.0]
     Community (ro): [common]
     Trap Recipient's IP address in dot notation: [0.0.0.0]
     Community (ro): [FibreChannel]
     Trap Recipient's IP address in dot notation: [0.0.0.0]

     SNMP access list configuration:
     Access host subnet area in dot notation: [0.0.0.0] 192.168.64.0
     Read/Write? (true, t, false, f): [true]
     Access host subnet area in dot notation: [0.0.0.0]
     Read/Write? (true, t, false, f): [true]
     Access host subnet area in dot notation: [0.0.0.0]
     Read/Write? (true, t, false, f): [true]
     Access host subnet area in dot notation: [0.0.0.0]
     Read/Write? (true, t, false, f): [true]
     Access host subnet area in dot notation: [0.0.0.0]
     Read/Write? (true, t, false, f): [true]
     Access host subnet area in dot notation: [0.0.0.0]
     Read/Write? (true, t, false, f): [true]
     Committing configuration...done.
     value = 1 = 0x1
```

To reset the SNMP agent configuration to default values, issue the `agtCfgDefault` command, as in the following example:

```
switch:admin> agtcfgdefault
*****
This command will reset the agent's configuration back to factory default
*****
Current SNMP Agent Configuration
Customizable MIB-II system variables:
          sysDescr = Fibre Channel Switch
       sysLocation = End User Premise
        sysContact = Field Support
  authTrapsEnabled = false

SNMPv1 community and trap recipient configuration:
  Community 1: Secret C0de (rw)
    No trap recipient configured yet
  Community 2: OrigEquipMfr (rw)
    No trap recipient configured yet
  Community 3: private (rw)
    No trap recipient configured yet
  Community 4: public (ro)
    No trap recipient configured yet
  Community 5: common (ro)
    No trap recipient configured yet
  Community 6: FibreChannel (ro)
    No trap recipient configured yet

SNMP access list configuration:
Entry 0:  Access host subnet area 192.168.64.0 (rw)]
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet

*****
Are you sure? (yes, y, no, n): [no]

Committing configuration...done.
agent configuration reset to factory default
Current SNMP Agent Configuration
Customizable MIB-II system variables:
          sysDescr = Fibre Channel Switch
       sysLocation = End User Premise
        sysContact = Field Support
  authTrapsEnabled = false
SNMPv1 community and trap recipient configuration:
  Community 1: Secret Code (rw)
    No trap recipient configured yet
  Community 2: OrigEquipMfr (rw)
    No trap recipient configured yet
  Community 3: private (rw)
    No trap recipient configured yet
  Community 4: public (ro)
    No trap recipient configured yet
  Community 5: common (ro)
    No trap recipient configured yet
  Community 6: FibreChannel (ro)
    No trap recipient configured yet
(output truncated)
```

To modify the options for configuring SNMP MIB traps, issue the `snmpmibcapset` command, as in the following example:

```
switch:admin> snmpmibcapset
The SNMP Mib/Trap Capability has been set to support
FE-MIB
SW-MIB
FA-MIB
SW-TRAP
FA-TRAP
FA-MIB (yes, y, no, n): [yes]
SW-TRAP (yes, y, no, n): [yes]
   swFCPortScn (yes, y, no, n): [no]
   swEventTrap (yes, y, no, n): [no]
   swFabricWatchTrap (yes, y, no, n): [no]
   swTrackChangesTrap (yes, y, no, n): [no]
FA-TRAP (yes, y, no, n): [yes]
   connUnitStatusChange (yes, y, no, n): [no]
   connUnitEventTrap (yes, y, no, n): [no]
   connUnitSensorStatusChange (yes, y, no, n): [no]
   connUnitPortStatusChange (yes, y, no, n): [no]
SW-EXTTRAP (yes, y, no, n): [no]
no change
switch:admin>
```

The following notes apply to the `snmpmibcapset` command parameters for FA-TRAP:

- connUnitStatusChange indicates that the overall status of the connectivity unit has changed. Its variables are:
  - connUnitStatus: the status of the connection unit
  - connUnitState: the state of the connection unit
- connUnitEventTrap indicates that the connectivity unit has generated an event. Its variables are:
  - connUnitEventId: the internal event ID
  - connUnitEventType: the type of this event
  - connUnitEventObject: used with the connUnitEventType to identify the object to which the event refers
  - connUnitEventDescr: the description of the event
- connUnitSensorStatusChange indicates that the status of the sensor associated with the connectivity unit has changed:
  - connUnitSensorStatus: the status indicated by the sensor
- connUnitPortStatusChange indicates that the status of the sensor associated with the connectivity unit has changed:
  - connUnitPortStatus: shows overall protocol status for the port
  - connUnitPortState: shows the user-specified state of the port hardware

To view the SNMP MIB trap setup, issue the `snmpmibcapshow` command, as in the following example:

```
switch:admin> snmpmibcapshow
FE-MIB: YES
SW-MIB: YES
FA-MIB: YES
SW-TRAP: YES
   swFCPortScn: NO
   swEventTrap: NO
   swFabricWatchTrap: NO
   swTrackChangesTrap: NO
FA-TRAP: YES
   connUnitStatusChange: NO
   connUnitEventTrap: NO
   connUnitSensorStatusChange: NO
   connUnitPortStatusChange: NO
SW-EXTTRAP: NO
switch:admin>
```

ISL trunking user guide

7

This chapter contains updates to the *HP StorageWorks ISL Trunking Version 3.1.x/4.1.x User Guide*, part number AA-RTSAC-TE.

In the section "Trunking Ports," in the third bullet on page 17, replace the following information:

ISL Trunking does not support the LE, L1, or L2 `portcfglongdistance` modes. For information about these modes and Extended Fabrics in general, refer to the *HP StorageWorks Extended Fabric Version 3.1.x/4.1.x User Guide*.

With this text:

ISL Trunking is supported for normal E_Ports (referred to as L0 in the `portcfglongdistance` command) with LWL media up to 5 km at the full speed permitted by the link. With LWL media, the throughput begins to fall off beyond 5 km, due to normal latency effects.

HP ISL Trunking for Fabric OS v3.2 supports LE, L0.5, L1, and LD modes (if the LD cable lengths are within the supported static mode ranges less than or equal to 50 km).

HP ISL Trunking for Fabric OS v3.2 does not support L2 mode.

For information about these modes and Extended Fabrics in general, refer to the *HP StorageWorks Extended Fabric Version 3.1.x/4.1.x User Guide*.

Add the following section at the end of Chapter 1:

Long-Distance Trunking

This section provides information on long-distance trunking between Fabric OS v3.2 switches, including the SAN Switch 2/8 EL and SAN Switch 2/16. Long-distance ISL trunking is a new feature for Fabric OS v3.2.x and Fabric OS v4.4.0.

Long-Distance Trunking Requirements

Requirements for ISL Trunking and Extended Fabrics in Fabric OS v3.2.x are as follows:

- The ISL Trunking and Extended Fabrics licenses are required.
- All trunk group ports must be part of the same quad.
- All trunk group ports must be running at 2 Gbit/sec. ISL Trunking does not support 1 Gbit/sec speeds.
- All trunk group ports must have similar deskew values.
- ISL Trunking is automatically enabled between adjacent switches that support trunking.
- All trunking ports in the same trunk group should be configured to be the same Extended Fabrics distance (for example, LD - LD, L0.5 - L0.5, or L1 - L1).
- As the distance increases, more buffer credits are needed, and fewer ports can form a trunk group.
- SAN Switch 2/8 EL and SAN Switch 2/16 ASICs limit buffer allocation to 63 maximum per port, so long-distance trunks can be established only up to this buffer limit.

Long-Distance Trunking Summary

The following is a summary of SAN Switch 2/8 EL and SAN Switch 2/16 long-distance settings and supported distances:

- L0 less than or equal to 5 km and a 2-, 3-, or 4-port trunk group (normal distance trunking allocates 26 buffer credits across 4 data VCs)
- LE less than or equal to 10 km and a 2-, 3-, or 4-port trunk group (allocates 19 buffer credits across VC2)
- L0.5 less than or equal to 25 km and a 2- or 3-port trunk group (allocates 29 buffer credits across VC2)
- L1 less than or equal to 50 km and a 2-port trunk group (allocates 54 buffer credits across VC2)
- L2 less than or equal to 100 km (no trunking support)
- LD less than or equal to 100 km (trunking supported at distances under 50 km)

Fabric OS reference guide

8

This chapter contains updates to the *HP StorageWorks Fabric OS Version 3.1.x/4.1.x Reference Guide*, part number AA-RS24C-TE.

New and modified commands for Fabric OS v3.2.x:

- `aaaconfig` (new for v3.2.x)
- `agtcfgshow`
- `authutil`
- `configdownload`
- `configure`
- `fabretryshow`
- `fabricshow`
- `fabstatsshow`
- `fwportdetailshow` (new for v3.2.x)
- `fwset` (new for v3.2.x)
- `fwshow`
- `pathinfo`
- `passwd`
- `perfmonitorclear` (new for v3.2.x)
- `perfmonitorshow` (new for v3.2.x)
- `perfshoweemonitor`
- `portcfggport`
- `portcfgislmode`
- `portcfglongdistance`
- `portcfglport`
- `portshow`
- `quietmode`
- `secauthsecret` (new for v3.2.x)
- `secmodeenable`
- `snmpmibcapset`

- `snmpmibcapshow`
- `switchshow`
- `switchstatusshow`
- `tempshow`
- userconfig (new for v3.2.x)
- `zonecreate`
- `zoneobjectcopy` (new for v3.2.x)
- `zoneobjectexpunge` (new for v3.2.x)
- `zoneobjectrename` (new for v3.2.x)

aaaconfig

Configures the RADIUS server settings.

Syntax

`aaaconfig [“--`*`actions`*`”]`

Availability

Admin

Description

Use this command to accomplish the following:

- Display the current RADIUS configuration.
- Add and delete new RADIUS servers.
- Modify an existing RADIUS server configuration.
- Enable and disable the RADIUS configuration.

The configuration applies to a single switch instance only.

Operands

This command has the following operands:

`--show`
Lists current RADIUS configurations. This information includes the RADIUS servers, port numbers, protocol, and so forth. The operand appears whether or not the RADIUS and switch database configuration are enabled.

`--add server_IP`
Adds a new RADIUS server. The minimum required field is the IP address of the server. All other fields use defaults: port to 1812, timeout to 3 seconds, and protocol to CHAP. The server is added to the end of the list. No more than five RADIUS servers can be configured.

`--remove server_IP`
Deletes the specified RADIUS server, if it exists.

```
--change server_IP
[-p port]
[-s secret]
[-t timeout]
[-chap | -pap]
```
Changes the specified server attributes. The operand `server_IP` is mandatory. If any attributes are specified, they are updated.

`--move` *`server_IP to_position`*
Moves the specified server to a specific position in the list of servers. The `--show` operand displays the current position of the servers.

```
--radius
[on | off]
```
Enables or disables the RADIUS configuration. If enabled, all login attempts are first attempted through the RADIUS servers configured. If disabled, the servers are not accessed and users are authenticated from the switch database.

`--switchdb [on | off]`
Enables or disables the switch database authentication. This option is closely tied to `--radius`. If RADIUS is off, this operand has no effect. If RADIUS is on, there are two options:

- `--switchdb off` implies the local authentication is not attempted, even if all of the RADIUS servers are inaccessible. This option disables users defined in the switch database from logging in to the switch. Use this option with restraint, because if none of the RADIUS servers is available, the switch becomes inaccessible to manage.
- `--switchdb on` implies that if all of the RADIUS servers are inaccessible, users are authenticated from the switch database. If the user is not defined in the switch database, login fails. For the default accounts like root, factory, admin, and user, the login is always from the switch database.

If no operands are specified, the command displays its usage.

Example

To display the usage:

```
switch:admin> aaaConfig
Usage: aaaConfig
--show:                       display current AAA service configuration
--add <server> [options]:     add a RADIUS server to configuration
--remove <server>:            remove a RADIUS server from configuration
--change <server> [options]:  change a RADIUS server configuration
--move <server> <to_position>:move a RADIUS server from the current position to the
new position
--radius <on | off>:          turn on/off current RADIUS configuration
--switchdb <on | off>:        turn on/off switch switch DB database as secondary
authentication
```

To display the current configuration:

```
switch:admin> aaaConfig "--show"

   Position   Server         Port  Secret       Timeout(s)   Auth-Protocol
   1         192.168.66.243  1812  sharedsecret     3           CHAP
   Primary AAA Service: RADIUS
   Secondary AAA Service: Switch database
```

To add a RADIUS server with default values:

```
switch:admin> aaaConfig "--add 10.64.245.138"
```

agtcfgshow

Displays the SNMP agent configuration.

Syntax

```
agtcfgshow
```

Availability

All users

Description

This command displays the configuration of the SNMP agent in the switch. The following fields are displayed:

`sysDescr` The system (switch) description (in MIB-II definition). The default value is `Fibre Channel Switch`.

`sysLocation` The location of the system (switch) (in MIB-II definition). The default value is `End User Premise`.

`sysContact` The contact information for this system (switch). The default value is `Field Support`.

`swEventTrapLevel` The event trap level with the event's severity level. When an event occurs, if its severity level is at or below the set value, the SNMP trap and swEventTrap is sent to configured trap recipients. By default, this value is set at `0`, which means that no swEventTrap is sent. Possible values are:

- 0 none
- 1 critical
- 2 error
- 3 warning
- 4 informational
- 5 debug

See `errshow` for related information.

`authTrapsEnabled` The authentication trap, authenticationFailure, is transmitted to the configured trap recipient when the agent receives a protocol message that is not properly authenticated. In the context of SNMPv1 and SNMPv2c, the agent receives a protocol message with an unmatched community string value. The factory default value is `false`.

In addition, there are six communities and respective trap recipients supported by the agent. The first three communities are for read-write access (`rw`) and the last three are for read-only access (`ro`).

For an SNMP management station to receive a trap generated by the agent, the administrator must configure a trap recipient value to correspond to the IP address of the management station.

There are six Access Control Lists (ACL) to restrict SNMP get and set operations to hosts under a host-subnet-area. Host-subnet-area is defined by comparing nonzero IP octets. For example, an ACL of `192.168.64.0` allows for access by any hosts that start with `192.168.64`, regardless of the fourth octet. ACL entries also have a flag to set each host-subnet-area to be read-write or read-only. The highest privilege matched out of six entries is given to the access.

ACL check is turned off when all six entries contain `0.0.0.0`.

Note: This command does not display the ACL in secure mode. When secure mode is enabled, the Access Control List feature is incorporated into the WSNMP and RSNMP security policies.

Operands

None

Example

To display the SNMP agent configuration:

```
switch:admin> agtcfgShow
     Current SNMP Agent Configuration
         Customizable MIB-II system variables:
                 sysDescr = FC Switch
              sysLocation = End User Premise
               sysContact = Field Support.
         swEventTrapLevel = 3
         authTrapsEnabled = true

     SNMPv1 community and trap recipient configuration:
       Community 1: Secret Code (rw)
         Trap recipient: 192.168.1.51
       Community 2: OrigEquipMfr (rw)
         Trap recipient: 192.168.1.26
       Community 3: private (rw)
         No trap recipient configured yet
       Community 4: public (ro)
         No trap recipient configured yet
       Community 5: common (ro)
         No trap recipient configured yet
       Community 6: FibreChannel (ro)
         No trap recipient configured yet

     SNMP access list configuration:
     Entry 0:  Access host subnet area 192.168.64.0 (rw)]
     Entry 1:  No access host configured yet
     Entry 2:  No access host configured yet
     Entry 3:  No access host configured yet
     Entry 4:  No access host configured yet
     Entry 5:  No access host configured yet
```

See Also

agtcfgset

agtcfgdefault

authutil

Manages authentication configuration.

Syntax

```
authutil [“--show”] | [“--set value”]
```

Availability

Admin

Description

Use this command to display and set local switch authentication parameters. Use the `--set` option to change authentication parameters, such as protocol and DH group. This saves the new configuration persistently. The authentication process uses the protocol that is set using this command.

When no protocol is set, the default setting is `all`; for example, `fcap, dhchap` is used. When no group is set, the default setting of `*`; for example, `0,1,2,3,4` is used. The new configuration is effective with the next authentication request.

Use the `--show` option to display the current authentication configuration of the switch. Use the `portshow` command to display the authentication type and associated parameters (if applicable) used on the port at port online or when enabling security (whichever was the most recent).

Note: A security license is required to run this command in both nonsecure and secure modes.

Operands

The operands are:

`--show` Displays local authentication configuration.

`--set` *`value`* Modifies authentication configuration. Values are:

- `-a` *`value`*, which sets authentication protocol. Specify `fcap` to set FCAP authentication only, `dhchap` to set DH-CHAP authentication only, and `all` to set FCAP and DH-CHAP (default). When authentication is set to `all`, implicit order is FCAP and then DH-CHAP; for instance, authentication negotiation FCAP is given priority over DH-CHAP on the local switch, but you can still select DH-CHAP.
- `-g` *`value`*, which sets Diffie-Hellman group (DH group). Values 0 through 4 and ***** are valid. DH group 0 is called NULL DH. Each DH group specifies a key size and associated parameters implicitly. A higher group value provides stronger cryptography and a higher level of security with the authentication protocol. When the DH group is set to a specified value, only that DH group is enabled in authentication. Specifying `*` as a group enables all DH groups (0, 1, 2, 3, and 4, in that order: default). For instance, authentication negotiation NULL DH is given priority over other groups, but you can still select other DH groups.

Examples

To display authentication configuration on the switch:

```
switch:admin> authutil "--show"
AUTH TYPE     HASH TYPE     GROUP TYPE
-----------------------------------------
fcap,dhchap    sha1,md5     0,1,2,3,4
```

To set DH-CHAP as the authentication protocol:

```
switch:admin> authutil "--set -a dhchap"
Committing configuration...done.
Authentication is set to dhchap.
```

To set both protocols, in order of FCAP and then DH-CHAP:

```
switch:admin> authutil "--set -a all"
Committing configuration...done.
Authentication is set to fcap,dhchap.
```

To set DH group 3:

```
switch:admin> authutil "--set -g 3"
Committing configuration...done.
DH Group is set to 3.
```

To set all DH groups to be specified in authentication negotiate order of 0, 1, 2, 3, and 4:

```
switch:admin> authutil "--set -g *"
Committing configuration...done.
DH Group is set to 0,1,2,3,4
```

See Also

`portshow`

`secauthsecret`

configdownload

Downloads the switch configuration from a host file.

Syntax

```
configdownload [”host”, ”user”, ”file” [, ”passwd”]]
```

Availability

Admin

Description

Use this command to download the switch configuration from a host file. The configuration file might have been generated previously using configupload, or it might have been created to download only specific configuration changes. See `configupload` for a description of the configuration file format.

The download process uses either file transfer protocol (FTP) or the RSHD protocol (TCP service 514). Both of these services are widely available on UNIX® hosts, but less so on Windows hosts.

On Windows NT®, the FTP server might have to be installed from the distribution media and enabled; on Windows NT or Windows 9x, there are several good freeware and shareware FTP servers available. To use RSHD on Windows NT or 9x, two utilities are supplied, RSHD.EXE and CAT.EXE, together with instructions on how to install and run them. The FTP server or RSHD must be running before a download can occur.

The command can be invoked without any parameters; in that case the user is prompted for input, including choice of FTP or RSHD. If invoked with three parameters, RSHD is used; otherwise, the presence of the fourth parameter (FTP password) selects FTP.

The download can fail for any of the following reasons:

- The switch has not been disabled.
- The host name is not known to the switch.
- The host IP address cannot be contacted.
- The user does not have permission on the host.
- The user runs a script that prints something at login.
- The file does not exist on the host.
- The file is not a switch configuration file.
- The RSHD or FTP server is not running on the host.
- The configuration data contains errors.

When the switch is in secure mode, the following rules and restrictions apply:

- Both defined security policies and active security policies sections must exist and contain the FCS_POLICY.
- In the defined security policies section, at least one member of the FCS_POLICY must be the same as a member in the previous FCS_POLICY.
- In the active security policies section, the FCS_POLICY must be exactly the same as the previous FCS_POLICY; order of members must be maintained.
- If either security policies section has an RSNMP_POLICY, that section must have a WSNMP_POLICY.
- After the switch is enabled, if the switch is the primary FCS, its security and zoning information is propagated to all other switches in the fabric.
- After the switch is enabled, if the switch is a non-FCS or a backup FCS, its security and zoning information are overwritten by the primary FCS.

Note: Security parameters and the switch's identity cannot be changed by configdownload. Parameters such as the switch's name and IP address are ignored; they are the lines in the configuration file that begin boot. Security parameters such as secure mode setting and version stamp are ignored; they are the lines in the configuration file that begin with sec.

A license key is accepted only if the boot.mac line matches the World Wide Name of the switch performing the download; otherwise, it is ignored.

The download process is additive; the lines read from the file are added to the current switch configuration. It is therefore possible to change a single configuration variable by downloading a file with a single line. All other variables remain unchanged.

This is particularly important when downloading a zoning configuration. Because the new zoning information is added to the current configuration, there cannot be any conflicts. If the current zoning configuration is to be replaced, the keyword clear might be inserted into the configuration file immediately before the zoning lines (start at the line [Zoning]).

If the configuration file contains keyword enable followed by a zoning configuration, that zoning configuration is enabled in the fabric. If there is no enable keyword in the configuration file, or no zoning configuration by that name exists, or if enable fails for any reason (such as dangling aliases):

- The effective configuration remains what it was before the configdownload; that is, all the enable statements are discarded.
- The defined configuration changes to reflect the new zoning configuration.

Operands

The following operands are optional:

host Host name or IP address in quotes; for example, citadel or 192.168.1.48. The configuration file is downloaded from this host.

user User name in quotes; for example, jdoe. This user name is used to gain access to the host.

file A file name in quotes: for example, config.txt. Absolute path names can be specified using a forward slash (/). Relative path names search for the file in the user's home directory on UNIX hosts and in the directory where the FTP or RSHD server is running on Windows hosts

passwd If present, selects FTP.

Example

To download a configuration file from host citadel, using account jdoe and file config.txt:

```
switch:admin> configDownload "citadel","jdoe","config.txt"
Committing configuration...done.
download complete
```

See Also

configdefault

configshow

configupload

configure

configure

Changes system configuration settings.

Syntax

```
configure
```

Availability

Admin

Description

Use this command to change system configuration settings, including:

- "Switch Fabric Settings" next
- "Virtual Channel Settings" on page 167
- "Zoning Operation Parameter" on page 168
- "RSCN Transmission Mode" on page 169
- "Arbitrated Loop Settings" on page 169
- "System Services Settings" on page 170
- "Portlog Events Disable and Enable Settings" on page 171
- "Application Attributes" on page 172

This command cannot be executed on an enabled system except for application attributes. The application attributes can be configured when the system is enabled; to configure any other settings, you must first disable the system, using the `switchdisable` command.

The `configure` command is navigated by entering a series of hierarchical menus. Each top-level menu and its associated submenus consists of a text prompt, a list of acceptable values (if appropriate), and a default value (shown in brackets). The default value is used with the carriage return, which is a special input case (see "Special Inputs" on page 172).

Switch Fabric Settings

There are a number of settings that control the overall behavior and operation of the fabric. Some of these values, such as the domain, are normally assigned by the fabric and may differ from one switch to another. However, other parameters, such as the buffer-to-buffer credit or the time out values, can be changed to suit particular applications or operating environments, but must be in agreement among all switches to allow formation of the fabric.

Table 13 defines the settings affecting the fabric that can be changed. Each field is described following the table.

Table 13: Switch Fabric Settings

Field	Type	Default	Range
Domain	Number	1	Varies
BB Credit	Number	16	1 to 27
R_A_TOV	Number	10000	E_D_TOV * 2 to 120000
E_D_TOV	Number	2000	1000 to R_A_TOV / 2
WAN_TOV	Number	0	0 to R_A_TOV / 4
MAX_HOPS	Number	7	7 to 19
Data Field Size	Number	2112	256 to 2112
Sequence-Level Switching	Boolean	0	0 or 1
Disable Device Probing	Boolean	0	0 or 1
Suppress Class F Traffic	Boolean	0	0 or 1
SYNC IO Mode	Boolean	0	0 or 1
VC Encoded Address Mode	Boolean	0	0 or 1
Disable Translative Mode	Boolean	0	0 or 1
Switch PID Format	Number	1	0 to 2
Per-Frame Route Priority	Boolean	0	0 or 1
Long-Distance Fabric	Boolean	0	0 or 1

Domain

The domain number uniquely identifies the switch in a fabric. Normally, this value is automatically assigned by the fabric. The range of allowed values varies depending on the switch model and other system settings (see “VC Encoded Address Mode” on page 166).

BB Credit

The buffer-to-buffer (BB) credit represents the number of buffers available to attached devices for frame receipt.

R_A_TOV

The resource allocation timeout value (R_A_TOV) is displayed in milliseconds. This variable works with the E_D_TOV variable to determine the switch actions when presented with an error condition.

Allocated circuit resources with detected errors are not released until the time value has expired. If the condition is resolved before the timeout, the internal timeout clock resets and waits for the next error condition.

E_D_TOV

The error detect timeout value (E_D_TOV) is displayed in milliseconds. This timer is used to flag a potential error condition when an expected response is not received (an acknowledgment or reply in response to packet receipt, for example) within the set time limit. If the time for an expected response exceeds the set value, an error condition is met.

WAN_TOV

The wide area network timeout value (WAN_TOV) is displayed in milliseconds. This timer is the maximum frame timeout value for a WAN, if any, interconnecting the Fibre Channel islands.

MAX_HOPS

Maximum hops (MAX_HOPS) is an integer. It denotes the upper limit on the number of hops a frame might have to hop to reach any destination port from any source port across the fabric.

Note: The configure parameters R_A_TOV, E_D_TOV, WAN_TOV, and MAX_HOPS are interrelated. Assigning a specific value to one or more of these parameters might change the range of values that can be assigned to the other parameters. As a result, the user might not be able to set all the values within the range displayed for each parameter. To make it easier, the configure utility validates the modified values of these four parameters and prompts the user to reenter them if the validation check fails.

Data Field Size

This specifies the largest possible value, in bytes, for the size of a type 1 (data) frame. The switch advertises this value to other switches in the fabric during construction of the fabric, as well as to other devices when they connect to the fabric. Setting this to a value less than 2112 might result in decreased performance.

Sequence-Level Switching

When this feature is set to 1, frames of the same sequence from a particular source are transmitted as a group. When set to 0, frames are transmitted interleaved among multiple sequences.

Under normal conditions, sequence level switching should be disabled for better performance. However, some host adapters have performance issues when receiving interleaved frames from multiple sequences. When there are such devices attached to the fabric, sequence level switching should be enabled.

Disable Device Probing

When this is set, devices that do not register themselves with the Name Server are not present in the Name Server database. Set this mode only if the switch's N_Port discovery process (PLOGI, PRLI, INQUIRY) causes some attached device to fail.

Suppress Class F Traffic

By default, the switch can send Class F frames. When this operand is turned on, Class F traffic is converted to Class 2 traffic before being transmitted.

SYNC IO Mode

By default, SYNC IO mode is disabled. When the option is enabled, tasks on the local switch wait for a response to its request from the remote switch before proceeding further. This option is enabled in the remote fabric environment to assist the detection of link failure.

VC Encoded Address Mode

When this mode is set, frame source and destination addresses utilize an address format compatible with some first-generation switches. Set this mode only if the fabric includes such switches.

Note: VC encoded address mode cannot be set in security mode. When this mode is set, security mode cannot be enabled.

Disable Translative Mode

The setting is relevant only if VC encoded address mode is also set. This feature, when set, disables translative addressing to achieve explicit address compatibility with some first-generation switches. Set this feature only if hardware or software systems are attached to the fabric that explicitly rely on a specific frame address format.

Switch PID Format

The setting is relevant only if VC encoded address mode is not set:

- `0` Native PID format (16 based, 16 port format), for fabrics with legacy low-count-port switches
- `1` Core PID format (0 based, 256 port format), preferred mode for mixed fabrics with legacy and new switches
- `2` Extended-edge PID format (16 based, 256 port format), used in mixed fabrics with legacy and new switches to avoid rebooting host systems when static PID binded is used

If VC encoded address mode is not set, the default setting is 1.

Note: The `configdefault` command does not change switch PID format.

Per-Frame Route Priority

In addition to the eight virtual channels used in frame routing priority, support also is available for per-frame-based prioritization when this value it set. When set, the virtual channel ID is used with a frame header to form the final virtual channel ID.

Long-Distance Fabric

When this mode is set, ISLs in a fabric can be up to 100 km. The exact distance is determined by the per-port configuration on the E_Ports of each ISL. Both E_Ports in an ISL must be configured to run the same long-distance level; otherwise, the fabric segments.

The Extended Fabrics license is required to set this mode.

Virtual Channel Settings

The switch provides the ability to tune the switch in a specific application by configuring the parameters for the switch's eight virtual channels. The first two virtual channels are reserved for the switch's internal functions and are not user configurable.

The default virtual channel settings have already been optimized for switch performance. Judiciously changing the default values might improve switch performance somewhat, but can also severely degrade performance. You should not change these settings without fully understanding the effects. See Table 14 for the virtual channel settings. Each field is described after the table.

Table 14: Virtual Channel Settings

Field	Type	Default	Range
VC Link Control	Number	0	0 to 1
VC Class 2	Number	2	2 to 5
VC Class 3	Number	3	2 to 5
VC Multicast	Number	7	6 to 7
VC Priority 2	Number	2	2 to 3
VC Priority 3	Number	2	2 to 3
VC Priority 4	Number	2	2 to 3
VC Priority 5	Number	2	2 to 3
VC Priority 6	Number	3	2 to 3
VC Priority 7	Number	3	2 to 3

VC Link Control

Specifies the virtual channel used for N_Port-generated, Class 2 link control frames (ACKs, P_BSYs, P_RJTs). Forces N_Port-generated link control frames to be sent, using a Class 2 data virtual channel when set to 0. When set to 1, the control frames are sent using a virtual channel normally reserved for fabric-internal traffic.

This setting is configurable only when VC encoded address mode is set.

VC Class 2

Specifies the virtual channel used for Class 2 frame traffic. This setting is configurable only when VC encoded address mode is set.

VC Class 3

Specifies the virtual channel used for Class 3 frame traffic. This setting is configurable only when VC encoded address mode is set.

VC Multicast

Specifies the virtual channel used for multicast frame traffic. This setting is configurable only when VC encoded address mode is set.

VC Priority

Specifies the class of frame traffic given priority for a virtual channel.

Zoning Operation Parameter

Table 15 specifies the zoning operation parameter. The field is described following the table.

Table 15: Zoning Operation Parameter

Field	Type	Default	Range
Disable Nodename Zone Checking	Boolean	0	0 or 1

Disable Nodename Zone Checking

By default, zoning uses both port WWN and node WWN to perform zoning. When the option is set to `1`, node WWN cannot be used in zoning.

RSCN Transmission Mode

Table 16 provides the RSCN transmission mode values. Each field is described following the table.

Table 16: RSCN Transmission Mode

Field	Type	Default	Range
End-Device RSCN Transmission Mode	Number	1	0 to 2
Domain RSCN-to-End Device for Switch IP Address or Name Change	Number	0	0 to 1

End-Device RSCN Transmission Mode

End-device RSCN transmission mode values are:

- `0` RSCN contains only a single PID.
- `1` RSCN contains multiple PIDs.
- `2` Fabric address RSCN.

Domain RSCN-to-End Device for Switch IP Address or Name Change

Domain RSCN to end-device for switch IP address or name change values are:

- `0` Disabled. No domain RSCN is sent to the end device for a switch IP address change or a name change.
- `1` Enabled. Domain RSCN is sent to the end device for a switch IP address change or a name change.

Arbitrated Loop Settings

Table 17 defines settings affecting Fibre Channel arbitrated loops that can be changed. Each field is described after the table.

Table 17: Arbitrated Loop Settings

Field	Type	Default	Range
Send FAN frames?	Boolean	1	0 or 1
Always send RSCN?	Boolean	0	0 or 1
Enable CLOSE on OPEN Received?	Number	4	0 to 4
Do Not Allow AL_PA 0x00?	Boolean	0	0 or 1
Initialize All Looplets?	Boolean	0	0 or 1

Send FAN frames?

Specifies whether fabric address notification (FAN) frames are sent to public loop devices to notify them of their node ID and address. When set to 1, such frames are sent; when set to 0, such frames are not sent.

Always send RSCN?

Following the completion of loop initialization, a remote state change notification (RSCN) is issued only when FL_Ports detect the presence of new devices or the absence of preexisting devices. When this feature is set, an RSCN always is issued following the completion of loop initialization, regardless of the presence or absence of new or preexisting devices.

Enable CLOSE on OPEN Received?

There are compatibility issues between tachLite-based products and switches with Enable CLOSE on OPEN Received. Multiple options are introduced to work around this issue and there is a known *Open Deadlock* defect, which has become part of legacy code. Preferred default is 4. See Table 18 for possible values. Each field is described after the table.

Table 18: Enable CLOSE on OPEN Received Values

Value	Enable CLS on OPN	Open Deadlock
0	0 (tachLite compatible)	Not fixed
1	1	Not fixed
2	0 (tachLite compatible)	Firmware fix
3	1	Firmware fix
4	1	Hardware fix

Do Not Allow AL_PA 0x00?

Some loop devices do not operate well with AL_PA 0 on the same loop. This option provides a workaround for such devices. By default, the switch can use a phantom AL_PA 0 for an embedded port in a QuickLoop configuration. When set to 1, the switch does not use AL_PA 0.

Initialize All Looplets?

By default, only looplets in the same zone are reinitialized. When set to 1, the option forces a reinitialization of all the looplets in the QuickLoop.

System Services Settings

Table 19 provides the system services settings. Each field is described following the table.

Table 19: System Services Settings

Field	Type	Default	Range
rstatd	Boolean	0	0 or 1
rusersd	Boolean	0	0 or 1

Table 19: System Services Settings (Continued)

Field	Type	Default	Range
rapid	Boolean	1	0 or 1
thad	Boolean	1	0 or 1
Disable RLS Probing	Boolean	1	0 or 1

rstatd

Dynamically enables or disables a server that returns information through remote procedure calls (RPCs) about system operation. The protocol provides for a wide range of system statistics; however, only the Ethernet interface statistics (see `ifshow`) and system up time (see `uptime`) are supported.

The retrieval of this information is supported by a number of operating systems that support RPC. On most UNIX-based systems (HP-UX, Irix, Linux, Solaris, and so forth), the commands to retrieve the information are rup and rsysinfo. Refer to your local system documentation for the appropriate usage of the `rup`, `rsysinfo`, or equivalent commands.

rusersd

Dynamically enables or disables a server that returns information via remote procedure calls (RPC) about the user logged into the system. The information returned includes the user login name, the system name, the login protocol or type, login time, idle time, and remote login location (if applicable).

The retrieval of this information is supported by a number of operating systems that support RPC. On most UNIX-based systems (HP-UX, Irix, Linux, Solaris, and so forth), the command to retrieve the information is rusers. Refer to your local system documentation for the appropriate usage of the `rusers` or equivalent command.

rapid

Dynamically enables or disables API service.

thad

Dynamically enables or disables Fabric Watch service.

Disable RLS Probing

Enables or disables FCP RLS (read link state) information probing for an F/FL_Port. It is disabled by default.

Portlog Events Disable and Enable Settings

Use this setting to disable logging port events. The default is on (enabled). When disabled, this event is not logged by port log.

Special Inputs

Special inputs are:

`Carriage return` When entered alone at a prompt without any preceding input, the command accepts the default value (if applicable) and moves to the next prompt.

`Interrupt` Aborts the command immediately and ignores all changes made.

`End-of-file` When entered alone at a prompt without any preceding input, terminates the command and saves any changes.

Application Attributes

HTTP, SNMP, and RPCd are configurable. By default, all three attributes are enabled. Table 20 specifies the attributes for applications that can be changed.

Table 20: Configure Application Attributes

Application	Field	Type	Default	Range
http	HTTP Enabled	Boolean	1	0 or 1
snmp	SNMP Enabled	Boolean	1	0 or 1
rpcd	RPCd Enabled	Boolean	1	0 or 1

Operands

None

Example

To configure:

```
switch:admin> configure

     Configure...

  Fabric parameters (yes, y, no, n): [no] y

    Domain: (1..239) [1]
    BB credit: (1..27) [16]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    WAN_TOV: (0..30000) [0]
    MAX_HOPS: (7..19) [7]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    SYNC IO mode: (0..1) [0]
    VC Encoded Address Mode: (0..1) [0]
    Switch PID Format : (0..2) [1]
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]

  Virtual Channel parameters (yes, y, no, n): [no] y

    VC Priority 2: (2..3) [2]
    VC Priority 3: (2..3) [2]
    VC Priority 4: (2..3) [2]
    VC Priority 5: (2..3) [2]
    VC Priority 6: (2..3) [3]
    VC Priority 7: (2..3) [3]

  Zoning Operation parameters (yes, y, no, n): [no] y

    Disable NodeName Zone Checking: (0..1) [0]

  RSCN Transmission Mode (yes, y, no, n): [no] y

    End-device RSCN Transmission Mode
      (0 = RSCN with single PID, 1 = RSCN with multiple PIDs, 2 = Fabric RSCN): (0..2) [1]
    Domain RSCN To End-device for switch IP address or name change
      (0 = disabled, 1 = enabled): (0..1) [0]

  Arbitrated Loop parameters (yes, y, no, n): [no] y

    Send FAN frames?: (0..1) [1]
    Always Send RSCN?: (0..1) [0]
    Enable CLOSE on OPEN received?: (0..4) [4]
    Do Not Allow AL_PA 0x00?: (0..1) [0]
    Initialize All Looplets?: (0..1) [0]
System services (yes, y, no, n): [no] y

    rstatd (on, off): [off]
    rusersd (on, off): [off]
    rapid (on, off): [on]
    thad (on, off): [on]
    Disable RLS probing (on, off): [on]

(continued on next page)
```

```
Portlog events enable (yes, y, no, n): [no] y
            start(a switch start or re-start event   )    (on, off): [on]
          disable(a port is disabled                 )    (on, off): [on]
           enable(a port is enabled                  )    (on, off): [on]
            ioctl(a port I/O control is executed)    )    (on, off): [on]
               Tx(a frame is transmitted)            )    (on, off): [on]
              Tx1(a frame is transmitted, class 1    )    (on, off): [on]
              Tx2(a frame is transmitted, class 2    )    (on, off): [on]
              Tx3(a frame is transmitted, class 3    )    (on, off): [on]
               Rx(a frame is received                )    (on, off): [on]
              Rx1(a frame is received, class 1       )    (on, off): [on]
              Rx2(a frame is received, class 2       )    (on, off): [on]
              Rx3(a frame is received, class 3       )    (on, off): [on]
            stats(port status or statistics          )    (on, off): [on]
              scn(a state change notification        )    (on, off): [on]
           pstate(a port changes physical state      )    (on, off): [on]
           reject(a received frame is rejected       )    (on, off): [on]
             busy(a received frame is busied         )    (on, off): [on]
             ctin(a CT based request is received     )    (on, off): [on]
            ctout(a CT based response is transmitted )    (on, off): [on]
           errlog(a message is added to the error log)    (on, off): [on]
          loopscn(a loop state change notification   )    (on, off): [on]
           create(a task is created                  )    (on, off): [on]
            debug(generic debug info                 )    (on, off): [on]
           nbrfsm(neighbor state transition          )    (on, off): [on]
            timer(timer                              )    (on, off): [on]
               sn(speed negotiation state            )    (on, off): [on]
           nsRemQ(inter-sw NS query                  )    (on, off): [on]
           nsRemR(inter-sw NS response               )    (on, off): [on]
             rscn(RSCN                               )    (on, off): [on]
          reconf(fabric reconfiguration              )    (on, off): [on]
          LR1(                                    LR2)    (0n, off): [off]

 Configure Application Attributes:

  http:
       HTTP Enabled (yes, y, no, n): [yes]

  snmp:
       SNMP Enabled (yes, y, no, n): [yes]

  rpc:
       RPCd Enabled (yes, y, no, n): [yes]

         Committing configuration...done.
```

See Also

agtcfgdefault

agtcfgshow

agtcfgset

configdefault

configshow

ifshow

ipaddrset

portcfgislmode

switchdisable

switchenable

uptime

fabretryshow

Displays the retry count of the fabric commands.

Syntax

```
fabretryshow
```

Availability

All users

Description

Use this command to display the retry count of various fabric commands. The first line of output displays SW_ISL, the ISL ports.

The subsequent lines display the retry count for the following fabric commands:

ELP	Exchange link parameters
EFP	Exchange fabric parameters
DIA	Domain identifier assigned
RDI	Request domain identifier
BF	Build fabric
RSCN	Remote state change notification
FWD	Fabric controller forward
EMT	Fabric controller mark timestamp
ETP	Exchange trunking parameters
GAID	Get address identifier
INQ	Inquiry command

Operands

None

Example

To display the retry count of the fabric commands:

```
switch:user> fabretryshow

                             E_Ports
     SW_ILS         0       1       2       3       4       5       6       7


     ELP            0       0       0       0       0       0       0       0

     EMT            0       0       0       0       0       0       0       0

     ETP            0       0       0       0       0       0       0       0

     EFP            0       0       0       0       0       0       0       0

     DIA            0       0       0       0       0       0       0       0

     RDI            0       0       0       0       0       0       0       0

     BF             0       0       0       0       0       0       0       0
```

See Also

fabstatsshow

fabricshow

Displays fabric membership information.

Syntax

`fabricshow`

Availability

All users

Description

Use this command to display information about switches and multicast alias groups in the fabric. Multicast alias groups are created only on demand by requests from N_Ports attached to the alias server, so typically no groups are listed.

If the switch is initializing or disabled, the message `no fabric` is displayed. If the fabric is reconfiguring, some or all switches might not appear; otherwise, the following fields are displayed:

`Switch ID`	The switch's Domain_ID and embedded port D_ID.
`World Wide Name`	The switch's World Wide Name.
`Enet IP Addr`	The switch's FC IP address.
`FC IP Addr`	The switch's FC IP address.
`Name`	The switch's symbolic name (> indicates the principal switch).

If any multicast alias groups exist, the following fields are displayed:

`Group ID`	The alias group number and D_ID.
`Token`	The alias group token (assigned by the N_Port)

Operands

None

Example

To display a fabric of four switches (sw180 is the principal switch, three of the switches are configured to run IP over Fibre Channel, and there is one multicast alias group):

```
switch:admin> fabricShow
  Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr      Name
  -------------------------------------------------------------------------
    1: fffc41 10:00:00:60:69:00:02:0b  192.168.64.180  192.168.65.180 >"sw180"
    2: fffc42 10:00:00:60:69:00:05:91  192.168.64.60   192.168.65.60   "sw60"
    3: fffc43 10:00:00:60:69:10:60:1f  192.168.64.187  0.0.0.0         "sw187"
    4: fffc40 10:00:00:60:69:00:06:56  192.168.64.59   192.168.65.59   "sw5"

  The Fabric has 4 switches

  Group ID    Token
  -----------------
    0: fffb01 40:05:00:00:10:00:00:60:69:00:00:15
```

See Also

switchshow

fabstatsshow

Displays the fabric statistics information.

Syntax

```
fabstatsshow
```

Availability

All users

Description

Use this command to display the statistics information for the fabric. The following information is displayed:

- Number of times a switch domain ID was forcibly changed
- Number of E_Port offline transitions
- Number of fabric reconfigurations
- Number of fabric segmentations due to:
  - Loopback
  - Incompatibility
  - Overlap
  - Platform DB
  - Sec Incompatibility
  - Security Violation
  - ECP Error
  - Duplicate WWN
  - E_Port Isolated

Operands

None

Example

To display the fabric statistics:

```
switch:user> fabstatsshow
    Description                    Count  Port  Time
    ---------------------------------------------------------------
    Domain ID forcibly changed:        0
    E_Port offline transitions:        47    5
    Reconfigurations:                  302   5  FRI MAR 19 18:36:30 2004
    Segmentations due to:
                         Loopback:     0
                  Incompatibility:     0
                          Overlap:     0
                           Zoning:     1 <      FRI MAR 19 18:36:30 2004
                          Routing:     0
                        Licensing:     0
                 Disabling E_Port:     0
         Incompatible platform DB:     0
               Security violation:     0
         Security incompatibility:     0
                   Eport Isolated:     0
```

See Also

fabretryshow

fwportdetailshow

Displays the overall status of the ports specified.

Syntax

fwportdetailshow ["--p", "*portNumber*"] | ["--s", "*portState*"]

Availability

All users

Description

Use this command to display the overall status of the ports specified. The overall status is calculated based on the following contributors:

- Port Errors:
  - LFA Number of link loss occurrences exceeded limit for time period.
  - LSY Number of sync loss occurrences exceeded limit for time period.
  - PER Number of protocol errors exceeded limit for time period.
  - INW Number of invalid words exceeded limit for time period.
  - CRC Number of invalid CRC errors exceeded limit for time period.
  - PSC Port hardware state changed too often.

- SFP Errors:
  - STMSFP temperature is out of specification.
  - SRXSFP receive power is out of specification.
  - STXSFP transmit power is out of specification.
  - SCUSFP current is out of specification.
  - SVOSFP voltage is out of specification.

The overall status can be in one of the following:

- HealthyEvery contributor is healthy.
- MarginalOne or more contributors are in this status.
- DownOne or more contributors are in this status.

If the overall status is not healthy, the contributing factors are displayed also.

Operands

If no operands are specified, all ports are displayed. The following operands are supported:

`--p` *`portNumber`* Yields a port detail report for a specific port.

`--s` *`portState`* Yields a port detail report for the specified *`portState`*. Valid *`portState`* entries are:

- `h`: Report based on all healthy ports.
- `m`: Report based on all marginal ports.
- `f`: Report based on all faulty ports.
- `o`: Report based on all offline ports.

Example

To display the port information for specified ports:

```
vxTarget:admin> fwportDetailShow
    Port Detail Report                          Report time: 07/23/2003 10:34:48 PM
    Switch Name:    vxTarget
    IP address:     192.168.204.82
    Port Exception report [by All]

    --------Port-Errors-------- -----SFP-Errors----
    Port# Type  State   Dur(H:M) LFA LSY LSI PER INW CRC PSC STM SRX STX SCU SV0
    --------------------------------------------------------------------------------
    000    U   OFFLINE   000:08   -   -   -   -   -   -   -   -   -   -   -   -
    001    U   OFFLINE   000:08   -   -   -   -   -   -   -   -   -   -   -   -
    002    U   OFFLINE   000:08   -   -   -   -   -   -   -   -   -   -   -   -
    003    U   OFFLINE   000:08   -   -   -   -   -   -   -   -   -   -   -   -
    004    LB  HEALTHY   000:08   -   -   -   -   -   -   -   -   -   -   -   -
    005    U   OFFLINE   000:08   -   -   -   -   -   -   -   -   -   -   -   -
    006    U   OFFLINE   000:08   -   -   -   -   -   -   -   -   -   -   -   -
    007    U   OFFLINE   000:08   -   -   -   -   -   -   -   -   -   -   -   -
    value = 0
```

See Also

`switchstatuspolicyshow`

`switchstatuspolicyset`

fwset

Sets parameters controlled by Fabric Watch.

Syntax

```
fwset ["--message", "mlevel"] | ["--port", "--persistence",
"seconds"]
```

Availability

All users

Description

Use this command to set parameters controlled by Fabric Watch. It allows the user to set the message level (severity of messages that are sent to the console) and the port persistence time (time in which a port must persistently be in a marginal state before being labeled as such).

Operands

The following operands are supported:

`--message` *`mlevel`*

Sets a filter for the messages sent to the console. Messages must be of the set severity level or higher in order to be output to the console. The value `-1` turns off all output to the console. Valid mlevel values are:

- `-1` = turn off console logging
- `0` = only panic messages to console
- `1` = critical and above messages to console
- `2` = error and above messages to console
- `3` = warning and above messages to console
- `4` = info and above messages to console
- `5` = debug and above messages to console

`--port --persistence` *`seconds`*

Sets port parameters. Currently, only port persistence time can be set with this operand. Port persistence time is the time period in which a port must be persistently in a state before being actually recognized as such.

Examples

To turn off console logging:

```
switch:admin> fwSet "--message", "-1"
```

To set the port persistence time to 18 seconds:

```
switch:admin> fwSet "--port", "--persistence", "18"
```

fwshow

Displays the thresholds monitored by Fabric Watch.

Syntax

```
fwshow ["--message"] | ["--port", "--persistence"]
```

Availability

All users

Description

If no parameters are entered, a summary of all thresholds is displayed. If a valid threshold name is entered as a parameter, detailed information pertaining only to that threshold is displayed.

Note: This command requires a Fabric Watch license.

Operands

The following operands are supported:

`--port --persistence`
Currently, `--port` has only one action, which is `--persistence`. This is the time that a port must be persistently in a state before being marked as such.

`--message`
Displays the severity levels of the messages being sent to the console.

Examples

To display the thresholds monitored by Fabric Watch:

```
switch:admin> fwShow
     =========================================================================
     Name                  Label                     Last value
     ----------------      ------------------------  -----------------------------
     envTemp001            Env Temperature 1                 33 C
     envTemp002            Env Temperature 2                 33 C
     envTemp003            Env Temperature 3                 36 C
     envTemp004            Env Temperature 4                 35 C
     envTemp005            Env Temperature 5                 36 C
     envFan001             Env Fan 1                       5070 RPM
     envFan002             Env Fan 2                       3090 RPM
     envFan003             Env Fan 3                       3150 RPM
     envFan004             Env Fan 4                       5130 RPM
     envPS002              Env Power Supply 2                 0 (1 OK/0 FAULT
```

To display valid thresholds named `envTemp001`:

```
switch:admin> fwShow "envTemp001"

     Env Temperature 1:

        Monitored for:       1283 (21 mins)
         Last checked:   10:50:21 on 02/01/2000

          Lower bound:          0 C
          Upper bound:         75 C
          Buffer Size:         10

        Value history:         33 C

             Disabled? No
               Locked? No
```

To display valid thresholds named `envTemp`:

```
switch:admin> fwShow "envTemp*"
     =========================================================================
     Name               Label                      Last value
     ----------------   ------------------------   -----------------------------
     envTemp001         Env Temperature 1                31 C
     envTemp002         Env Temperature 2                35 C
     envTemp003         Env Temperature 3                37 C
     envTemp004         Env Temperature 4                37 C
     envTemp005         Env Temperature 5                37 C
```

To display the console level:

```
switch:admin> fwShow "--message"
FW: console level set to 5
```

To display the current port persistence time:

```
switch:admin> fwShow "--port", "--persistence"
FW: current port persistence time = 18s
```

See Also

`fwclassinit`
`fwconfigreload`
`fwconfigure`

pathinfo

Displays routing and statistics information along a path.

Syntax

```
pathinfo [[[domain], source port], destination port] [,"-r"]
```

Availability

Admin

Description

Use this command to display detailed routing information from a source port (or area) on the local switch to a destination port (or area) on another switch. This routing information describes the exact path that a user data stream takes to go from the source to the destination. If the user specifies the use of inactive ports or a path through a switch that does not have active routing tables to the destination, pathinfo describes the path that is used if the ports were active. If the user specifies a destination port that is not active, pathinfo uses the embedded port as the destination.

For switches with blades, the ingress and egress points are specified as area numbers. For a nonbladed switch, ingress and egress points are specified as ports. This agrees with the representation in the `switchshow` command.

In addition, pathinfo can provide, upon request, statistics on every traversed ISL.

Routing and statistics information is provided by every switch along the path, based on the current routing tables and statistics calculated continuously in realtime. Each switch represents one hop.

Other options allow the collection of information on the reverse path or on a user-selected path (source route).

For each hop, the routing information output consists of the following:

`Hop` The hop number; the local switch is hop 0.

`In Port` The port (or area) from which the frames come. For hop 0, the source port. For a switch with blades, this is specified as the area number; otherwise, it is the port number.

`Domain ID` The domain ID of the switch.

`Name` The name of the switch.

`Out Port` The output port that the frames take to reach the next hop. For the last hop, the destination port or area. For a switch with blades, this is specified as the area number; otherwise, it is the port number.

`BW` The bandwidth of the output ISL, in Gbit/sec. It does not apply to the embedded port.

`Cost` The cost of the link used by FSPF routing protocol. It applies only to an E_Port.

For each hop, statistics are divided into *basic* and *extended*. They are reported below the routing information, separated into *input* port statistics and *output* port statistics. For each port, they are further separated into *transmit* and *receive* statistics. Statistics are not reported for the embedded port.

Some values are measured over multiple time intervals. For example, the output line utilization in bytes per second is calculated over both a 1-second period and over a 64-second period. This gives an idea of both the current line utilization and the utilization over a longer period of time. The time interval is reported in parenthesis after the value's description.

Maximum hop count

The `pathinfo` command uses a special frame that is sent hop-by-hop from the source switch to the destination switch, collecting routing and statistics information at every hop. To prevent such a frame from looping forever if an error occurs, a maximum number of hops for the frame to hop is enforced. The hop count includes all hops in the direct path from source to destination, and also all the hops in the reverse path, if tracing of the reverse path is requested. The default value for the maximum hop count is 25.

Basic statistics

Basic statistics report variables that give an indication of ISL congestion along the path. They consist of the following:

`B/s` Bytes per second

`Txcrdz` The length of time, in milliseconds, that the port was prevented from transmitting frames due to lack of buffer-to-buffer credit. It is an indication of downstream congestion. Other commands, such as portstatsshow, can express this value in units other than milliseconds.

Extended statistics

Extended statistics report variables are:

`F/s` Frames per second

`Words` Total number of 4-byte Fibre Channel words

`Frames` Total number of frames

`Errors` Total number of errors that might cause a frame not to be received correctly. This includes CRC errors, bad EOF errors, frame truncated errors, frame too short errors, and encoding errors inside a frame.

Reverse path

The path from port A on switch X to port B on switch Y might be different from the path from port B to port A. The difference could be in the links traversed between the same sequence of switches, or the reverse path might even involve different switches. The trace reverse path option allows the user to determine both routing and statistics information for the reverse path, in addition to those for the direct path.

Source route

The source route option allows the user to specify a sequence of switches or ports (or areas) that the pathinfo frame has to follow to reach the destination. Therefore, the path might be different from the one the actual traffic from source to destination takes.

The source route is expressed as a sequence of switches, a sequence of output ports (or areas), or a combination thereof. The next hop in the source route is described by either the output port (or area) to be used to reach the next hop or the domain ID of the next hop.

The source route can specify a partial route from source to destination (in which case the remaining hops are chosen as the path from the input port or area on the first hop not listed in the source route to the destination), as a full route, or as an arbitrary route across the fabric. The maximum hop count is enforced.

If the source route does not specify all the switches along a section of the path, a further option allows you to specify a *strict* versus a *loose* path. A strict source route requires that only the specified switches are reported in the path description. If two switches are specified back-to-back in the source route descriptor but are not directly connected, the switches in between are ignored. In case of a loose source route, the switches in between are reported. The concepts of strict and loose route apply to the portions of the path described by domains, not to the part described by output ports or areas.

Operands

The following operands are allowed:

`domain` The ID of the destination domain.

`source port` The port (or area) whose path to the destination domain is sought. The embedded port (`-1`) is used by default. For a switch with blades, the destination is specified as the area; otherwise, it is the port. If the source port is given as `-1`, with no additional arguments, basic statistics are displayed for the route.

`destination port` A port on the destination switch. pathinfo returns the state of the port (or area). The embedded port (`-1`) is used by default, or if the user specifies a destination port that is not active. For a switch with blades, the destination is specified as the area; otherwise, it is the port.

`-r` Displays the reverse path, in addition to the forward path, in the output.

Without operands, `pathinfo` is an interactive command in which the following parameters can be provided:

`max hops` The maximum number of hops that the pathinfo frame is allowed to traverse. Default: `25`.

`domain` The ID of the destination domain; mandatory, no default.

`source port` The port whose path to the destination domain is sought. It can be an F_Port or an E_Port. The embedded port (`-1`) is used by default. For a switch with blades, this is specified as the area; otherwise, it is the port.

`destination port` A port on the destination switch. The `pathinfo` command returns the state of the port, and all requested statistics pertaining to the port. The embedded port (`-1`) is used by default, or if the specified destination port is not an existing active port. For a switch with blades, this is specified as the area, otherwise the port.

`basic stats` Requests the reporting of basic statistics on every link; default is `no`.

`extended stats` Requests the reporting of extended statistics on every link; default is `no`.

`trace reverse path` Provides path information from the destination port to the source port; default is `no`.

`source route`: Specifies a sequence of switches or ports that the pathinfo frame should hop. Note that if an output port (or area) to the next hop is specified, the user is not prompted for the domain of the next switch that is determined by the port (or area) specified. Default: `no`.

`strict source rte` Specifies that the source route must be followed strictly as indicated, skipping possible intermediate switches. When using this option, the source route must be specified using domain numbers (rather than the output port).

`Timeout` The maximum time allowed to wait for the response; default is `10` seconds.

Examples

To invoke `pathinfo` with all operands on the command line:

```
switch:admin> pathInfo 91

     Target port is Embedded

     Hop  In Port  Domain ID (Name)      Out Port    BW   Cost
     ---------------------------------------------------------
      0       E         9 (web226)          2       1G   1000
      1       3        10 (web229)          8       1G   1000
      2       8         8 (web228)          9       1G   1000
      3       6        91 (web225)          E       -      -
```

To invoke pathinfo through the menu, including basic and extended statistics:

```
switch:admin> pathInfo

         Max hops: (1..127) [25]
         Domain: (1..239) [-1] 8
         Source port: (0..15) [-1]
         Destination port: (0..255) [-1]
         Basic stats (yes, y, no, n): [no] y
         Extended stats (yes, y, no, n): [no] y
         Trace reverse path (yes, y, no, n): [no]
         Source route (yes, y, no, n): [no]
         Timeout: (1..30) [5]


     Target port is Embedded

     Hop  In Port  Domain ID (Name)      Out Port    BW   Cost
     ---------------------------------------------------------
      0       E         9 (web226)           2       1G   1000

     Port                              E                             2
                              Tx             Rx             Tx             Rx
                              -----------------------------------------------
     B/s (1s)                  -              -              0              0
     B/s (64s)                 -              -              1              1
     Txcrdz (1s)               -              -              0              -
     Txcrdz (64s)              -              -              0              -
     F/s (1s)                  -              -              0              0
     F/s (64s)                 -              -           2743              0
     Words                     -              -        2752748        2822763
     Frames                    -              -         219849          50881
     Errors                    -              -              -              0

     Hop  In Port  Domain ID (Name)      Out Port    BW   Cost
     ---------------------------------------------------------
      1       3        10 (web229)          12       1G   1000

(continued on next page)
```

```
Port                              3                            12
                         Tx             Rx             Tx             Rx
                         -----------------------------------------------
B/s (1s)                 36             76              0              0
B/s (64s)                 5              5              5              5
Txcrdz (1s)               0              -              0              -
Txcrdz (64s)              0              -              0              -
F/s (1s)                  1              1              0              0
F/s (64s)                 0              0              0              0
Words             240434036        2294316        2119951        2121767
Frames             20025929          54999         162338          56710
Errors                    -              4              -              0

Hop  In Port  Domain ID (Name)      Out Port    BW   Cost
---------------------------------------------------------
 2      14         8 (web228)           E       -      -

Port                             14                             E
                         Tx             Rx             Tx             Rx
                         -----------------------------------------------
B/s (1s)                  0              0              -              -
B/s (64s)                 5              5              -              -
Txcrdz (1s)               0              -              -              -
Txcrdz (64s)              0              -              -              -
F/s (1s)                  0              0              -              -
F/s (64s)                 0              0              -              -
Words              20158695        1021842              -              -
Frames              1665662          56849              -              -
Errors                    -              4              -              -
```

See Also

portstatsshow

switchshow

passwd

Changes system passwords.

Syntax

passwd [*“login_name”*]

Availability

All users

Description

Use this command to change the password for users.

When used with the optional `login_name` operand, the command prompts the user to change the password only for that user. Otherwise, the command prompts the user to change passwords for the current user.

In either case, the user is first prompted for the old password. If the password entered matches the current password, the user is then prompted twice for the new password. The new password has to be different from the current password.

If the two copies do not match, the process is repeated at most two more times until the command fails for that user.

Passwords must be constructed to meet the following requirements:

- Each password must contain 8 to 40 characters.
- If the switch fabric is in secure mode, the command can run only on the primary switch. The changed password database is distributed to all FCS switches. Non-FCS switches are updated if the password of the user account is changed.
- The command is disabled until the user has changed all login passwords from the manufacturer’s defaults or the switch was in secure mode before.
- If a user is authenticated by RADIUS and invokes this command, the password of the account to which the user's role is mapped is changed. For example, if user `Bob`’s login role is mapped to `admin`, when Bob executes the `passwd` command, he changes the password of the `admin` account on the switch, provided Bob knows the old password for the `admin` account. The RADIUS account does not change.

Special Inputs

This command has the following special inputs:

`Carriage return`	When entered alone at a prompt without any preceding input, accepts the default value (if applicable) and moves to the next prompt.
`Interrupt`	Aborts the command immediately and ignores all changes made.
`End-of-file`	When entered alone at a prompt without any preceding input, terminates the command, saving any changes made.

Note: It is no longer possible to change a login name.

Operand

The following operand is optional:

`login_name`	The name of the user, in quotes, for which the login name and password are to be changed.

Example

To change the admin password:

```
switch:admin> passwd "admin"
Old password:
New password:
Re-enter new password:

Committing configuration...done.
```

Diagnostics

All error messages are preceded by the command name and followed by one of the following messages:

`“user” is not a valid user name.`	The user name was not a valid, recognized user name on the system.
`Permission denied.`	The current user does not have permission to change the user name or password for the specified user.
`Incorrect password.`	The user has not entered the correct password when prompted for the old password.
`Password unchanged.`	The user has entered the carriage return special input case, skipping the entire password change process.
`Number of failure attempts exceeded.`	The user has made three unsuccessful attempts to enter and verify a new password.
`Passwords do not match; try again.`	The user has not correctly verified the new password.

See Also

`login`

`logout`

perfmonitorclear

Clears statistics counters of end-to-end, filter-based, and ISL monitors on a port.

Syntax

```
perfmonitorclear “monitor_class”, port [, monitorId]
```

Description

Use this command to clear statistics counters for different classes of monitor. Monitor classes include end-to-end monitors (EE), filter-based monitors (FLT), and interswitch link (ISL) monitors. For end-to-end and filter-based counters, a monitor ID can be specified to clear only a particular monitor on a port. Use the `perfmonitorclear` command to ensure that the correct monitor counters are cleared.

After a successful execution of this command, the telnet shell confirms that this monitor's counters have successfully been cleared.

Issuing the `portstatsclear` command on a port also results in all monitors being cleared for all the ports in the same quad.

Operands

This command has the following operands:

monitor_class The monitor class, which can be one of EE (end-to-end), FLT (filter-based), or ISL (interswitch link).

port Specifies the port number in which to clear the counters. This operand is required.

monitorId Specifies the monitor number to clear. Monitor numbers are defined when you create the monitor on a port. This operand is optional. If not specified, all monitor counters on the port are cleared. This argument does not apply to ISL monitors.

Examples

To clear statistics counters for an end-to-end monitor:

```
switch:admin> perfMonitorClear "EE", 2, 5
End-to-End monitor number 5 counters are cleared
```

To clear statistics counters for a filter-based monitor:

```
switch:admin> perfMonitorClear "FLT", 4, 0
Monitor 0 counters are cleared
```

To clear statistics counters for an ISL monitor:

```
switch:admin> perfMonitorClear "ISL", 0
This will clear ISL monitor on port 0, continue? (yes, y, no, n): [no] y
ISL monitor on port 0 is cleared
```

See Also

perfmonitorshow

perfmonitorshow

Displays end-to-end, filter-based, and interswitch link (ISL) monitors on a port.

Syntax

perfmonitorshow “*monitor_class*”, *port* [, *interval*]

Availability

All users

Description

Use this command to display previously created monitors on a port. Monitor classes include end-to-end monitors (EE), filter-based monitors (FLT), and ISL monitors (ISL).

For end-to-end monitors, when an interval is not specified or 0 is specified, the command displays the 64-bit cumulative transmit counter (TX_COUNT), the receive counter (RX_COUNT) in Fibre Channel words (4 bytes), and the 33-bit CRC error counters in hexadecimal format. When a nonzero interval is specified in seconds, the command displays a rolling table of CRC, Tx, and Rx counters on per-interval basis for all the valid monitors on the port, in the units of bytes.

For filter-based monitors, when an interval is not specified or 0 is specified, the command displays only the 64-bit frame in hexadecimal. When a nonzero interval is specified, for each monitor on the port, a rolling table of cumulative frame counts is displayed, in decimal, for each monitor.

For ISL monitors, the command displays the 64-bit cumulative ISL transmit counter, 64-bit cumulative transmit counter for each individual domain, the total number of domains being monitored, and the number of ports in this ISL.

Operands

This command has the following operands:

monitor_class Specifies the monitor class: EE (end-to-end), FLT (filter-based), or ISL (interswitch link).

port Specifies the port number in which to display the end-to-end monitors. This operand is required.

interval Specifies the interval, in seconds. This operand is optional.

Examples

To display end-to-end monitors on port 3:

```
switch:admin> perfMonitorShow "EE", 3

There are 2 end-to-end monitor(s) defined on port 3.

KEY     SID     DID       OWNER_APP       OWNER_IP_ADDR      TX_COUNT          RX_COUNT           CRC_COUNT
-------------------------------------------------------------------------------------------------------------------
 0   0xb1300   0xb23ef   TELNET                N/A      0x0000000000000000  0x000000000025ad4f  0x0000000000000000
 1   0xb1200   0xb22ef   TELNET                N/A      0x0000000000000000  0x000000000025ad4f  0x0000000000000000
```

To display all end-to-end monitors on port 3 for every second (in this example, there are two monitors on port 3: 0, 1):

```
switch:admin> perfMonitorShow "EE", 3, 1

Showing EE monitors 3, 1: Tx/Rx are # of bytes and crc is # of crc errors

         0            1
  -------------  -------------
   crc  Tx   Rx  crc  Tx   Rx
  =============  =============
   0    0  1.2k  0    0  1.2k
   0    0  272   0    0  272
   0    0  136   0    0  136
   0    0  272   0    0  272
   0    0  272   0    0  272
   0    0  204   0    0  204
   0    0  204   0    0  204
   0    0  136   0    0  136
   0    0  272   0    0  272
   0    0  272   0    0  272
```

To display filter-based monitors on port 4:

```
switch:admin> perfMonitorShow "FLT", 4

     There are 2 filter-based monitors defined on port 4.

     KEY   ALIAS   OWNER_APP       OWNER_IP_ADDR     FRAME_COUNT
     ------------------------------------------------------------------
      0  SCSI_Frame TELNET               N/A      0x0000000000000000
      1  SCSI_RD    TELNET               N/A      0x0000000000000000
```

To display filter-based monitors on port 4 for every second (in this example, there are two monitors on port 4, 0 and 1):

```
switch:admin> perfMonitorShow "FLT", 4, 1

     Showing filter monitors 4, 1

           0       1
        #Frames   #CMDs
     ------------------
           0        0
           0        0
           0       10
         20k        0
           0        0
```

To display ISL monitors on port 7 (in this example, there is one port in this ISL; 16 domains are monitored because there are routes going to these domains by way of this ISL):

```
switch:admin> perfmonitorshow "ISL", 7

     Total transmit count for this ISL:       21748 g   780204495
     Number of destination domains monitored: 16
     Number of ports in this ISL: 1
     Domain  84:                        0     Domain  88:                  0
     Domain  89:                        0     Domain  90:                  0
     Domain  91:                        0     Domain  92:                  0
     Domain  95:      21748 g   780182720     Domain  96:                104
     Domain 100:                       36     Domain 102:                  0
     Domain 105:                        0     Domain 110:                  0
     Domain  80:                      112     Domain  81:              21299
     Domain  82:                      112     Domain  83:                112
```

See Also

perfaddeemonitor

perfaddusermonitor

perfshoweemonitor

Displays user-defined end-to-end monitors on a port.

Syntax

```
perfshoweemonitor port [, interval]
```

Note: This command is deprecated. The `perfmonitorshow` command should be used instead.

Availability

All users

Description

Use this command to display previously defined end-to-end monitors on a port. When an interval is not specified or 0 is specified, the command displays the 64-bit cumulative transmit counter (TX_COUNT), receive counter (RX_COUNT) in Fibre Channel words (4 bytes), and the 33-bit CRC error counters in hexadecimal format. When a nonzero interval is specified in seconds, the command displays a rolling table of CRC, Tx and Rx counters on a per-interval basis for all the valid monitors on the port, in the units of bytes.

End-to-end monitor monitors the traffic on receiving port. See `perfaddeemonitor` for more details on how to specify a monitor you want.

Operands

This command has the following operands:

`port` Specify the port number where you want to display the end-to-end monitors. This operand is required.

`interval` Specify the interval in second to monitor CRC_COUNT (CRC), TX_COUNT (Tx) and RX_COUNT (Rx). Tx and Rx are in unit of byte. This operand is optional.

Examples

To display EE monitors on port 3:

```
switch:admin> perfShowEEMonitor 3

There are 2 end-to-end monitor(s) defined on port 3.

KEY     SID     DID       OWNER_APP       OWNER_IP_ADDR      TX_COUNT          RX_COUNT           CRC_COUNT
-------------------------------------------------------------------------------------------------------------------
 0   0xb1300   0xb23ef    TELNET                N/A      0x0000000000000000  0x000000000025ad4f  0x0000000000000000
 1   0xb1200   0xb22ef    TELNET                N/A      0x0000000000000000  0x000000000025ad4f  0x0000000000000000
```

To display all EE monitors on port 3 for every second (in this example, there are two monitors on port 3: 0, 1):

```
switch:admin> perfShowEEMonitor 3, 1
Showing EE Monitors 3, 1: Tx/Rx are # of bytes and crc is # of crc errors

         0            1
  -------------  -------------
   crc  Tx   Rx  crc  Tx   Rx
  =============  =============
   0    0  1.2k  0    0  1.2k
   0    0  272   0    0  272
   0    0  136   0    0  136
   0    0  272   0    0  272
   0    0  272   0    0  272
   0    0  204   0    0  204
   0    0  204   0    0  204
   0    0  136   0    0  136
   0    0  272   0    0  272
   0    0  272   0    0  272
```

See Also

perfaddeemonitor

perfdeleemonitor

portcfggport

Locks a port as a G_Port.

Syntax

`portcfggport *port_number*, *mode*`

Availability

Admin

Description

Use this command to designate a port as a G_Port. The switch then attempts to initialize that port as only a G_Port.

The switch never attempts loop (L_Port) initialization on the port.

The configuration is saved in nonvolatile memory and is persistent across a switch reboot or power cycle.

Operands

The following operands are required:

port_number The port number to be configured: 0 through 7 or 0 through 15.

mode A value of `1` means *port_number* is designated as a locked G_Port. A value of `0` means *port_number* is configured from its previous role as a locked G_Port.

Example

To configure switch port 3 as a locked G_Port:

```
switch:admin> portCfgGport 3, 1
Committing configuration...done.
```

See Also

`configure`

`portcfglport`

`portshow`

`switchshow`

portcfgislmode

Enables or disables port ISL R_RDY mode.

Syntax

`portcfgislmode` *`port_number`*`, [1 | 0]`

Availability

Admin

Description

Use this command to configure a port as ISL R_RDY mode enabled or disabled. When enabling ISL R_RDY mode and when the neighboring switch is of the same brand, the PID format between the switches must be the same.

Note: The `portcfgislmode` and `portcfglongdistance` modes cannot both be enabled at the same time; otherwise, the fabric segments.

Operands

This command has the following operands:

port_number The port number to be configured. This operand is required.

ISL R_RDY mode Set to `1` to enable. Set to `0` to disable. This operand is required.

Example

To configure port 3 to have ISL R_RDY mode disabled:

```
switch:admin> portCfgISLMode 3, 0
Committing configuration...done.
```

See Also

portcfgshow

portshow

switchshow

portcfglongdistance

Configures a port to support long-distance links.

Syntax

```
portcfglongdistance port_number,"long_distance_level"
[, VC_translation_link_initialization]
```

Availability

Admin

Note: This command requires the Extended Fabrics license.

Description

Use this command to allocate enough full-size frame buffers on a particular port to support a long-distance link up to 100 km. The port can be used as either an Fx_Port or an E_Port. The configuration is saved in nonvolatile memory and is persistent across switch reboots or power cycles.

When this command is invoked without user-supplied operands, the operands are assigned default values.

The long-distance level string must be one of the following:

`L0` Reconfigure the port to be a regular switch port. The number of buffers reserved for the port supports up to 10 km links at 1 Gbit/sec.

`LE` Level E mode is for E_Ports for distances beyond 5 km and up to 10 km. The number of buffers reserved for the port supports up to 10 km links at 1 Gbit/sec and 2 Gbit/sec. LE does not require an Extended Fabrics license.

`L0.5` Level 0.5 long distance, up to 25 km.

`L1` Level 1 long distance, up to 50 km.

`L2` Level 2 long distance, up to 100 km.

`LD` Dynamic long-distance configuration. The buffer credits for the given E_Port are automatically configured based on the actual link distance. Up to a total of 63 full-size frame buffers are reserved, depending upon the distance measured during E_Port initialization.

The VC (virtual channel) translation link initialization parameter must be set to 1 for long distance. When set to 1, this parameter indicates that the enhanced link reset protocol is used for long-distance links. When this parameter is not specified by the user, it is set to 1 by default. To be compatible with earlier Fabric OS v3.x implementations, 0 can be used for this parameter.

When a port is configured as a long-distance port, portCfgShow and `switchshow` output displays the long-distance level as Lx, where x is 0, 0.5, 1, 2, D, or E. The `portCfgShow` command also displays the current setting for the VC translation link initialization parameter.

Extended Fabrics mode is not supported when interoperable mode is enabled.

Note: The portcfgislmode and `portcfglongdistance` modes cannot both be enabled at the same time; otherwise, the fabric segments.

Operands

The following operand is required:

`port_number` The port number to be configured: 0 through 7 or 0 through 15.

The following operands are optional:

`long_distance_level` See the “Description” on page 199 section for the meaning of this value. The default value is `LD` (dynamic long distance).

VC_translation_link_init	See the “Description” on page 199 section for the meaning of this value. The default value is `1` when not specified with the long-distance setting. Therefore, the command `portcfglongdistance` *`port_number`* implies `portcfglongdistance` *`port_number`*`, LD, 1.`

Limitations

Because the total number of frame buffers is limited in a quad, if one of the ports in the quad is configured and enabled as an L2 long-distance port, all remaining ports are disabled due to the lack of sufficient buffer credits. Similarly, you also can configure an L1 long-distance port in combination with other port types provided there are sufficient buffer credits for the remaining ports in the quad. As an example, here are two valid port configurations: two L1 long-distance ports at 2 Gbit/sec speed, or four LE or three L0.5 long-distance ports at 2 Gbit/sec.

A quad is defined as a group of four adjacent ports that share a common pool of frame buffers. Ports 0 through 3 belong to a quad, as do ports 4 through 7, and so forth.

If the long-distance links are between StorageWorks 1 GB switches, in order to have a long-distance port take effect, all switches in the fabric must be configured to run the long-distance fabric mode (for instance, the long-distance fabric mode bit must be set to be 1). Otherwise, the fabric segments. In fact, you cannot configure a long-distance port in a switch unless the long-distance fabric mode is on for that switch.

For the same reason, when all ports are reconfigured to non-long-distance ports, you must reconfigure the long distance fabric mode for that switch.

This restriction does not apply to fabrics with long-distance links between StorageWorks 2 GB switches.

Configurations with long-distance links between 2000- and 3000-series switches are not supported.

Example

To configure switch port 3 to support a 100 km link:

```
switch:admin> portCfgLongDistance 3, "L2"
Committing configuration...done.
```

To configure the port for long distance, to support a 50 km link with enhanced link reset protocol:

```
switch:admin> portCfgLongDistance 3, "L1", 1
Committing configuration...done.
```

See Also

`configure`

`portcfgshow`

`portshow`

`switchshow`

portcfglport

Locks a port as an L_Port, with options to be private or enabled half-duplex mode.

Syntax

```
portcfglport port_number, mode [,mode1] [,mode2]
```

Availability

Admin

Description

Use this command to designate a port as an L_Port. The switch then attempts to initialize only that port as an FL_Port. By default, the L_Port is a public L_Port. It can be set as a private L_Port and the FLOGI is rejected.

The switch never attempts point-to-point (F_Port) initialization on the port.

Operands

The following operands are required:

`port_number` The port number to be configured: 0 through 7 or 0 through 15.

`mode` A value of `1` means *`port_number`* is a locked L_Port. A value of `0` means *`port_number`* is deconfigured as a locked L_Port.

`mode1` If not specified, set to 0 by default.

- 1 The L_Port is a private L_Port; FLOGI is rejected.
- 0 The L_Port is a public L_Port.

`mode2` If *`mode2`* is not specified, set to 0 by default.

- 2 The L_Port is full-duplex mode with fairness ON.
- 1 The L_Port is half-duplex mode ON.
- 0 The L_Port is half-duplex mode OFF.

When the *`port_number`* operand is present, the *`mode`* operand must be the second parameter.

Without any operand, the command reports a list of ports and their current settings.

If the port under configuration is a QuickLoop port, all three modes are required when using portcfglport to configure this loop port to be half-duplex: for example, `portcfglport` *`port_number`*, *`mode`*, *`mode1`*, *`mode2`*.

Example

To configure switch port 3 as a locked L_Port:

```
sw5:admin> portCfgLport 3, 0, 1, 1
Committing configuration...done.

sw5:admin> portCfgLport
Ports:     0   1   2   3   4   5   6   7
        --------------------------------
Lock       -   -   -   -   -   -   -   -
Private    -   -   -   YES -   -   -   -
Loop HD    -   -   -   YES -   -   -   -
Fairness   -   -   -   -   -   -   -   -
```

To configure switch port 5:

```
sw5:admin> portCfgLport 5, 0, 0, 2
     Committing configuration...done.

sw5:admin> portCfgLport
     Ports:     0   1   2   3   4   5   6   7
               --------------------------------
     Lock       -   -   -   -   -   -   -   -
     Private    -   -   -   YES -   -   -   -
     Loop HD    -   -   -   YES -   -   -   -
     Fairness   -   -   -   -   -   YES -   -
```

See Also

`configure`

`portshow`

`switchshow`

portshow

Displays port status.

Syntax

`portshow` *`port_number`*

Availability

All users

Description

Use this command to display port status information. Some information varies with the switch model and port type. The output displays the following:

`portName` A user-assigned name for the port.

`portHealth` The current health of the port (Fabric Watch license required). States are:

- HEALTHY
- MARGINAL
- FAULTY
- OFFLINE

`Authentication` Authentication type and associated parameters (if applicable) used on the port at port online or when enabling security (whichever happened last). States are:

- None: No authentication was done.
- FCAP: FCAP authentication was done.
- DHCHAP: DH-CHAP authentication was done. Also displays DH group and hash used for authentication.

`portFlags` A bit map of port status flags.

`portType` The port's type and revision numbers.

`portState` The port's SNMP state:

- Online: Up and running
- Offline: Not online; portPhys gives details
- Testing: Running diagnostics
- Faulty: Failed diagnostics

`portPhys` The port's physical state:

- No_Card: No interface card present
- No_Module: No module (GBIC or other) present
- No_Light: The module is not receiving light
- No_Sync: Receiving light but out of sync
- In_Sync: Receiving light and in sync
- Laser_Flt: Module is signaling a laser fault
- Port_Flt: Port marked faulty
- Diag_Flt: Port failed diagnostics
- Lock_Ref: Locking to the reference signal

`portScn` The port's last State Change Notification.

`portRegs` Address of the port's hardware registers.

`portData`	Address of the port's driver private data.
`portId`	The port's 24-bit D_ID.
`portWwn`	The port's World Wide Name.
`portWwn of devices connected`	The World Wide Name of devices connected.
`Distance`	The port's long-distance level (see `portcfglongdistance`)

After the general information, there are three columns of counters. The first column displays interrupt statistics:

`Interrupts`	Total number of interrupts.
`Unknown`	Interrupts that are not counted elsewhere.
`Lli`	Low-level interface (physical state, primitive seqs).
`Proc_rqrd`	Frames delivered for embedded N_Port processing.
`Timed_out`	Frames that have timed out.
`Rx_flushed`	Frames requiring translation.
`Tx_unavail`	Frames returned from an unavailable transmitter.
`Free_buffer`	Free buffer available interrupts.
`Overrun`	Buffer overrun interrupts.
`Suspended`	Transmission suspended interrupts.
`Parity_err`	Real Tx data parity errors.
`2ndary_parity_err`	Secondary Tx data parity errors. These are not real Tx data parity errors, but rather forced by the ASIC due to certain central memory errors so that the transmitter aborts the frame. This field is displayed only when there are errors.

The second column displays Link Error Status Block counters:

`Link_failure` Number of times the port enters LF1 or LF2 state.

`Loss_of_sync` Number of times the port enters a loss of sync state.

`Loss_of_sig` Number of times the port enters a loss of signal state.

`Protocol_err` Number of occurrences of the link failure condition in which either an LR or LRR primitive sequence was received while in OL3 (wait for OLS) state.

`Invalid_word` Number of encoding/disparity errors inside of frames.

`Invalid_crc` Number of CRC errors.

`Delim_err` Number of SOF or EOF errors.

`Address_err` Number of IUs with a nonzero status received.

`Lr_in` Number of link reset requests received.

`Lr_out` Number of link reset requests sent out.

`Ols_in` Number of OLS Primitives received.

`Ols_out` Number of OLS Primitives sent out.

The third column displays the number of F_RJTs and F_BSYs generated. For L_Ports, the third column also displays the number of LIPs received, the number of LIPs transmitted, and the last LIP received.

`Frjt` Number of fabric reject messages sent out.

`Fbsy` Number of fabric busy messages sent out.

Operand

The following operand is required:

`port_number` The port number to be displayed: 0 through 7 or 0 through 15.

Example

To display an E_Port:

```
sw5:admin> portShow 3
portName:
portHealth: HEALTHY
Authentication: type DHCHAP, hash SHA1, group 0
portFlags: 0x28057 PRESENT ACTIVE E_PORT G_PORT U_PORT LOGIN LED
portType:  3.1
portState: 1Online
portPhys:  6In_Sync
portScn:   5E_Port
portRegs:  0x80000000
portData:  0x10fa9ef0
portId:    011300
portWwn:   20:03:00:60:69:00:00:10
portWwn of device(s) connected:         20:00:00:60:69:50:03:83
Distance:  normal
Speed:2Gbps
Interrupts:        15502      Link_failure: 0          Frjt:         0
Unknown:           0          Loss_of_sync: 2          Fbsy:         0
Lli:               12         Loss_of_sig:  1
Proc_rqrd:         15484      Protocol_err: 0
Timed_out:         0          Invalid_word: 0
Rx_flushed:        0          Invalid_crc:  0
Tx_unavail:        0          Delim_err:    0
Free_buffer:       0          Address_err:  0
Overrun:           1          Lr_in:        3
Suspended:         0          Lr_out:       1
Parity_err:        0          Ols_in:       1
2ndary_parity_err: 1   Ols_out:      3
```

See Also

authutil

portcfglongdistance

portstatsshow

switchshow

quietmode

Sets or clears shell quiet mode.

Syntax

`quietmode [`*`newMode`*`]`

Availability

All users (display)

Admin (set/clear)

Description

Use this command to affect the output displayed on the switch console (serial port or telnet session). Note that enabling quiet mode does not suppress the error log display that is controlled by syslog-related commands. Use the `syslog` command to determine the current error log settings.

By default, quiet mode is off and all switch tasks send output to the console. Some output is caused by asynchronous events, such as the fabric reconfiguring or by devices logging in.

When quiet mode is on, only output produced by shell commands is shown; all asynchronous output produced by other tasks is suppressed. This is useful when driving a telnet session by way of a script which cannot expect any asynchronous output. Error log messages are not controlled by quiet mode settings.

Operand

The *`newMode`* operand is optional:

- `0` clears quiet mode; all tasks are displayed.
- `1` sets quiet mode; only shell commands are displayed.

Example

The following command displays the current mode, which in this case is off, and then changes it to on:

```
switch:admin> quietMode
Quiet Mode is OFF
switch:admin> quietMode 1
Committing configuration...done.
Quiet Mode is now ON
```

See Also

`syslogshow`

secauthsecret

Displays, sets, or removes DH-CHAP secret key information.

Syntax

```
secauthsecret [“--actions”]
```

Availability

Admin

Description

Use this command to manage the DH-CHAP shared secret key database used for the authentication. Also use this command to display, set, and remove secret key information from the database or to delete the entire database. If performing a set or remove operation, when the command completes, new data is saved persistently. New data is effective with the next authentication request. The configuration applies to a switch instance only.

Operands

Without any specified action, the command displays the usage. Specify *`action`* as one of following:

`--show` Lists the WWNs for which the shared secret is configured.

`--set` Sets shared secrets with a WWN.

`--remove [wwn | domain | sw name]` Removes the specified WWN entry from the database. If a domain name is specified, it is converted to a WWN and then the entry is removed. If no option is specified, the command enters interactive mode.

`--remove --all` Deletes the entire secret key database.

Examples

To display the secret key information:

```
switch:admin> secAuthSecret "--show"

     WWN
     ---------
     10:00:00:60:69:80:05:14
```

To set the shared secrets with a WWN, interactively:

```
switch:admin> secAuthSecret "--set"

This command is used to set up secret keys for the DH-CHAP authentication.
The minimum length of a secret key is 8 characters and maximum 40
characters. Setting up secret keys does not initiate DH-CHAP
authentication. If switch is configured to do DH-CHAP, it is performed
whenever a port or a switch is enabled.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press Enter to start setting up shared secrets >

Enter WWN, Domain, or switch name (Leave blank when done): 10:00:00:60:69:80:05:14
Enter peer secret:
Re-enter peer secret:
Enter local secret:
Re-enter local secret:

Enter WWN, Domain, or switch name (Leave blank when done):
Are you done? (yes, y, no, n): [no] y
Saving data to key store... Done.
```

To remove all secret keys:

```
switch:admin> secAuthSecret "--remove --all"

This command deletes database of DH-CHAP secret keys. If a fabric
requires authentication, deleting this database may cause switch
to segment from the fabric.

Do want to remove secret key database? (yes, y, no, n): [no] y
Deleting secret key database... Done.
```

secmodeenable

Enables secure mode.

Syntax

```
secmodeenable [“--quickmode”] | [[“--currentpwd”]
[“--lockdown[=scc|=dcc]”][“--fcs list-of-switches” |
list-of-switches]]
```

Availability

Admin

Description

Use this command to enable secure mode on all switches in the fabric. The command fails if any switch in the fabric is not capable of enforcing the security policies defined in the security database. If no operand is specified, the command becomes interactive.

A secure telnet session (sectelnet or SSH) must be used to issue this command.

This command sets up security in the fabric by:

- Activating secure mode on all switches in the fabric.
- Creating the security database populated with a list of Fabric Configuration Server (FCS) switches in the FCS_POLICY.
- Distributing the security database to all switches in the fabric.
- Resetting the root, factory, admin, and user account passwords on all FCS switches in the fabric.
- Resetting the admin account password on all non-FCS switches in the fabric.
- Disabling the root and factory accounts on all non-FCS switches in the fabric.

The administrator is prompted to enter new passwords for the following accounts:

- root
- factory
- admin
- user
- non-FCS admin

The prompts do not appear if the administrator chooses to use the passwords on the primary FCS with the `--currentpwd` option. With this option, the admin password is used for non-FCS admin as well.

If the fabric is not in secure mode and one or more specified FCS switches are present in the fabric, the command must be issued on the first active FCS (primary FCS) in the list.

If the fabric is not in secure mode and this command is issued, switches in the fabric with versions earlier than v4.4 and earlier than v3.2 firmware, reboots automatically after the command is successfully executed.

If the fabric is not in secure mode and no specified FCS switches are present in the fabric, the command can be issued on any switch. Only the `--fcs` option can be used in this case.

Note: Ensure that all users (using Fabric OS CLI or Web Tools) are logged off the fabric before enabling secure mode. Users, whose account passwords are changed, are logged off once secure mode is enabled. The `--currentpwd` option uses the current passwords on the primary FCS; hence, users logged into the primary FCS are not logged off.

Operands

This command has the following operands:

`list-of-switches`
Specifies a list of switches for the FCS policy. The list of member switches must be enclosed in quotation marks and each member switch must be separated from the others by semicolons. The members can be specified using domain, WWN, or switch name format, as follows: `5; 10:00:00:60:69:00:00:20; star1.`

`--fcs` *`list-of-switches`*
Use the specified *`list-of-switches`* for the FCS policy. The *`list-of-switches`* is a semicolon-separated list of switches. The switches can be specified using domain, WWN, or switch name. Specifying `*` defaults to all the switches currently in the fabric.

`--currentpwd`
Use the current passwords of the switch the command is run on (the primary FCS switch) for root, factory, admin, and user accounts. A non-FCS admin account password is set the same as FCS admin account password. The command does not prompt for new passwords. Only sessions whose account password has changed are logged out. This option can be used only on a fabric with secure mode disabled and only when the command is run on the switch specified as the primary FCS switch.

`--lockdown [=scc|=dcc]`
Create SCC and DCC policies to lock down the fabric. SCC policies are populated with all the switches present in the fabric when the command was executed. DCC policies are populated with the devices present in the fabric when the command was executed, locking down devices on a per-port basis. Ports with no devices attached to them are also locked down with an empty DCC policy, so no device can be connected to them, preserving the fabric as is. The lockdown option creates both SCC and DCC policies; with the optional argument of `--lockdown=scc` or `--lockdown=dcc`, only the specified policy is created. This option can be used only on a fabric with secure mode disabled and only when the command is run on the switch specified as the primary FCS switch.

`--quickmode` Shorthand notation for a combination of the previous options; for example, `--currentpwd --lockdown --fcs *`. On successful execution of the command, security is enabled in the fabric. All switches are FCS and have passwords identical to that on the primary FCS, SCC, and DCC policies, capturing the current state of the fabric. This option can be used only on a fabric with secure mode disabled and only when the command is run on the switch specified as the primary FCS switch.

If a switch member is specified by domain or switch name, the switch must be in the fabric, or the command fails.

If the FCS list of switches is not specified, the session becomes interactive and the user is prompted to enter FCS members.

If the `--currentpwd` option is not used, the session becomes interactive and the user is prompted to enter new passwords for root, factory, admin, user, and non-FCS admin accounts.

All operands must be specified within double quotes.

Examples

To enable a security policy that includes three FCS switches specified by domain, WWN address, and switch name:

```
fcsprimary:admin> secmodeenable
Your  use of  the certificate-based  security features  of the  software
installed on this equipment is subject to the End User License Agreement
provided  with the equipment and the Certification  Practices Statement,
which you may review at http://www.switchkeyactivation.com/cps. By using
these security features, you are consenting to be bound by the  terms of
these  documents.  If you  do not agree to the terms of these documents,
promptly contact the entity from which you obtained this software and do
not use these security features.
Do you agree to these terms?  (yes, y, no, n): [no] y

This command requires Switch Certificate,  Security license and Zoning
license to be installed on  every switch in the fabric.

PLEASE NOTE: On successful completion of this command, login sessions might
be closed and some switches may go through a reboot to form a secure
fabric.
This is an interactive session to create a FCS list.

The new FCS list is empty.

Enter WWN, Domain, or switch name(Leave blank when done): 102
Switch WWN is 10:00:00:60:69:80:04:0f.

The new FCS list:
10:00:00:60:69:80:04:0f

Enter WWN, Domain, or switch name(Leave blank when done):
10:00:00:60:69:80:04:0e
Switch WWN is 10:00:00:60:69:80:04:0e.

The new FCS list:
10:00:00:60:69:80:04:0f
10:00:00:60:69:80:04:0e

Enter WWN, Domain, or switch name(Leave blank when done): sw1
Switch WWN is 10:00:00:60:69:80:04:0a.

The new FCS list:
10:00:00:60:69:80:04:0f
10:00:00:60:69:80:04:0e
10:00:00:60:69:80:04:0a

Enter WWN, Domain, or switch name(Leave blank when done):
Are you done?  (yes, y, no, n): [no] y
Is the new FCS list correct?  (yes, y, no, n): [no] y
Please enter current admin account password:

Warning:  Access to  the Root  and Factory accounts may be required  for
proper  support  of  the switch.  Please  ensure  the Root  and  Factory
passwords are  documented in a secure location.  Recovery of a lost Root
or Factory password will result in fabric downtime.

(continued on next page)
```

```
Changing password for root
New FCS switch root password:
Re-type new password:
Changing password for factory
New FCS switch factory password:
Re-type new password:
Changing password for admin
New FCS switch admin password:
Re-type new password:
Changing password for user
New fabric wide user password:
Re-type new password:
Changing password for admin
New Non FCS switch admin password:
Re-type new password:

Broadcast message from root Thu Feb 26 02:58:52 2004...

Security Policy or Password Change: root factory admin user will be
logged out on switch 0

Connection closed by foreign host.
user@hostmachine{238}%
```

To use the quick mode option:

```
fcsprimary:admin> secModeEnable "--quickmode"

Your  use of  the certificate-based  security features  of the  software
installed on this equipment is subject to the End User License Agreement
provided  with the equipment and the Certification  Practices Statement,
which you may review at http://www.switchkeyactivation.com/cps. By using
these security features, you are consenting to be bound by the  terms of
these  documents.  If you  do not agree to the terms of these documents,
promptly contact the entity from which you obtained this software and do
not use these security features.
Do you agree to these terms?  (yes, y, no, n): [no] y

This command requires Switch Certificate,  Security license and Zoning
license to be installed on  every switch in the fabric.

PLEASE NOTE: On successful completion of this command, login sessions
may be closed and some switches may go through a reboot to form a secure
fabric.

Non-FCS admin password will be set the same as FCS admin password.
ARE YOU SURE  (yes, y, no, n): [no] y

Please enter current admin account password:

Secure mode is enabled.
```

To use the current passwords option:

```
fcsprimary:admin> secModeEnable "--currentpwd --fcs *"

Your  use of  the certificate-based  security features  of the  software
installed on this equipment is subject to the End User License Agreement
provided  with the equipment and the Certification  Practices Statement,
which you may review at http://www.switchkeyactivation.com/cps. By using
these security features, you are consenting to be bound by the  terms of
these  documents.  If you  do not agree to the terms of these documents,
promptly contact the entity from which you obtained this software and do
not use these security features.
Do you agree to these terms?  (yes, y, no, n): [no] y

This command requires Switch Certificate,  Security license and Zoning
license to be installed on  every switch in the fabric.

PLEASE NOTE: On successful completion of this command, login sessions
may be closed and some switches may go through a reboot to form a secure
fabric.

Non-FCS admin password will be set the same as FCS admin password.
ARE YOU SURE  (yes, y, no, n): [no] y

Please enter current admin account password:

Secure mode is enabled.
```

See Also

secfabricshow

secmodedisable

secmodeshow

secpolicyshow

snmpmibcapset

Modifies options for configuring SNMP MIB trap capability.

Syntax

```
snmpmibcapset
```

Availability

Admin

Description

Use this command to turn on or off certain MIBs and traps. This command also enables a user to turn on or off group information and SSN in SW trap messages. It first displays current settings and then prompts the user to change the values for each parameter.

The snmpmibcapshow command displays the SNMP MIBs and TRAPs Capability of the SNMP agent in the switch:

FA-MIB	Specifying yes means the user can access FA-MIB variables with an SNMP manager. The default value is yes.
SW-TRAP	Specifying yes means the SNMP management application can receive SW-TRAPS from the switch. The default value is yes. Users can also turn on or off individual SW traps. The individual SW traps are swFCPortScn, swEventTrap, swFabricWatchTrap, and swTrackChangesTrap.
FA-TRAP	Specifying yes means the SNMP management application can receive FA-TRAPS from the switch. The default value is yes. Users can also turn on or off individual FA traps. The individual FA traps are connUnitStatusChange, connUnitEventTrap, connUnitSensorStatusChange, and connUnitPortStatusChange.
SW-EXTTRAP	Specifying yes means user can receive SSN in the SW traps. The default value is no.

Note: The agtcfgdefault command also resets the SNMP MIB and trap capability to default along with other SNMP agent configuration.

The values can be changed, if a user downloads the configuration data through the configdownload command.

All the new values successfully configured by the snmpmibcapset command take effect immediately.

If SNMP MIB is disabled, corresponding traps are disabled also. If any trap group is disabled, corresponding individual traps are disabled also.

The FE and SW MIBs are always accessible. The snmpmibcapset command does not prompt the user to turn on or off these MIBs.

Operands

None

Example

To set the SNMP MIB and trap capabilities of a switch:

```
Cylon51:admin> snmpmibcapset
The SNMP Mib/Trap Capability has been set to support
FE-MIB
SW-MIB
FA-MIB
SW-TRAP
   swFCPortScn
   swEventTrap
   swFabricWatchTrap
   swTrackChangesTrap
FA-TRAP
   connUnitStatusChange
   connUnitEventTrap
   connUnitSensorStatusChange
   connUnitPortStatusChange
FA-MIB (yes, y, no, n): [yes] n
SW-TRAP (yes, y, no, n): [yes]
   swFCPortScn (yes, y, no, n): [yes]
   swEventTrap (yes, y, no, n): [yes] n
   swFabricWatchTrap (yes, y, no, n): [yes]
   swTrackChangesTrap (yes, y, no, n): [yes] n
SW-EXTTRAP (yes, y, no, n): [no] y
Committing configuration...done.
```

See Also

agtcfgdefault

agtcfgset

agtcfgshow

snmpmibcapshow

Displays options for configuring SNMP MIB trap capability.

Syntax

```
snmpmibcapshow
```

Availability

All users

Description

Use this command to turn on or off certain MIBs and traps. This command also enables a user to turn on or off group information and SSN in SW trap messages. It first displays current settings and then prompts the user to change the values for each parameter.

The `snmpmibcapshow` command displays the SNMP MIBs and TRAPs Capability of the SNMP agent in the switch:

FA-MIB — Specifying yes means the user can access FA-MIB variables with an SNMP manager. The default value is `yes`.

SW-TRAP — Specifying yes means the SNMP management application can receive SW-TRAPS from the switch. The default value is `yes`. Users can also turn on or off individual SW traps. The individual SW traps are swFCPortScn, swEventTrap, swFabricWatchTrap, and swTrackChangesTrap.

FA-TRAP — Specifying yes means the SNMP management application can receive FA-TRAPS from the switch. The default value is `yes`. Users can also turn on or off individual FA traps. The individual FA traps are connUnitStatusChange, connUnitEventTrap, connUnitSensorStatusChange, and connUnitPortStatusChange.

SW-EXTTRAP — Specifying yes means user can receive SSN in the SW traps. The default value is `no`.

Note: The `agtcfgdefault` command also resets the SNMP MIB and trap capability to default along with other SNMP agent configuration.

The values can be changed, if a user downloads the configuration data through the `configdownload` command.

All the new values successfully configured by the `snmpmibcapset` command take effect immediately.

If SNMP MIB is disabled, corresponding traps are disabled also. If any trap group is disabled, corresponding individual traps are disabled also.

The FE and SW MIBs are always accessible. The `snmpmibcapset` command does not prompt the user to turn on or off these MIBs.

Operands

None

Example

To display the MIB and trap capabilities of a switch:

```
Cylon51:admin> snmpmibcapshow
FE-MIB: YES
SW-MIB: YES
FA-MIB: YES
SW-TRAP: YES
   swFCPortScn: YES
   swEventTrap: YES
   swFabricWatchTrap: YES
   swTrackChangesTrap: YES
FA-TRAP: YES
   connUnitStatusChange: YES
   connUnitEventTrap: YES
   connUnitSensorStatusChange: YES
   connUnitPortStatusChange: YES
SW-EXTTRAP: NO
```

See Also

agtcfgdefault

agtcfgset

agtcfgshow

switchshow

Displays switch and port status.

Syntax

`switchshow [“--`*`option`*`”]`

Availability

All users

Description

Use this command to display switch and port status information. Some information varies with the switch model: for instance, the number of ports and domain ID values. The lines of the output display the following:

`switchName`	The switch's symbolic name.
`switchType`	The switch's model and revision numbers.

`switchState` The switch's state: Online, Offline, Testing, or Faulty.

`switchMode` The switch's mode: Interop or Native.

`switchRole` The switch's role: Principal, Subordinate, or Disabled.

`switchDomain` The switch's Domain ID: 0 through 31 or 1 through 239.

`switchId` The switch's embedded port D_ID.

`switchWwn` The switch's World Wide Name.

`switchBeacon` The switch's beaconing state: either ON or OFF.

`Zoning` The switch's zoning state (either ON or OFF) and effective zone configuration, within parenthesis.

The switch summary is followed by one line per port:

`port number` The port number: 0 through 7 or 0 through 15.

`module type` The port module type (GBIC or other):

- — `No`: module present
- — `sw`: Shortwave laser
- — `lw`: Longwave laser
- — `cu`: Copper
- — `id`: Serial ID

Use the `gbicshow` command to display whether a serial ID GBIC is `sw`, `lw`, or `cu`.

`port speed` The port's link speed:

- — `1G`: Full speed, 1 Gbit/sec.
- — `2G`: Double speed, 2 Gbit/sec.
- — `AN`: Speed autonegotiation enabled.
- — `N1`: Speed negotiated to full speed.
- — `N2`: Speed negotiated to double speed.

`port state` The port's state:

- `No_Card`: No interface card present.
- `No_Module`: No module (GBIC or other) present.
- `No_Light:` The module is not receiving light.
- `No_Sync`: Receiving light but out of sync.
- `In_Sync`: Receiving light and in sync.
- `Laser_Flt`: Module is signaling a laser fault.
- `Port_Flt`: Port marked faulty.
- `Diag_Flt`: Port failed diagnostics.
- `Lock_Ref`: Locking to the reference signal.
- `Testing`: Running diagnostics.
- `Online`: The port is up and running.

`port distance` The port's long-distance mode. If a port is configured as a long-distance port, the long-distance level appears in the format `L`*`x`*, where *`x`* is the long-distance level number. See `portcfglongdistance` for the level description.

`comment` The comment field either can be blank or display:

- `Disabled`: The port is disabled.
- `Bypassed`: The port is bypassed (loop only).
- `Loopback`: The port is in loopback mode.
- `E_Port`: Fabric port; displays WWN of attached switch.
- `F_Port`: Point-to-point port; displays WWN of attached N_Port.
- `G_Port`: Point-to-point but not yet E_Port or F_Port.
- `L_Port`: Loop port; displays the number of NL_Ports.

`more comments` The comment field might have additional comments, depending on the comment field entry.

`Disabled` A disabled port might have additional comments that explain the reason for disabling it, such as Persistent or Security violation.

`L_Port` An L_Port indicates the number for public, private, and phantom devices in the loop.

`E_Port` An E_Port displays one or more of the following:

- WWN of the switch connected
- Switch name of the switch connected
- One or more interswitch link attributes
- Trunk master:
  - The port is the master port in a group of trunking ports.
- Trunk port, master is port #x:
  - The port is configured as a trunking port; the master port is port #x.
- Upstream:
  - This E_Port is an upstream path, towards the principal switch of the fabric.
- Downstream:
  - This E_Port is a downstream path, away from the principal switch of the fabric.

`F_Port` An F_Port displays the port WWN of the device attached to it.

Operand

The `-portcount` operand is optional; it causes the `switchshow` command to display the number of ports on the switch.

Examples

The following example displays a 16-port switch. Two ports are F_Ports (point-to-point connections to N_Ports), two ports are loop ports (one of which has eight private loop devices), and two ports are connected to another switch, sw6. If the optional -portcount operand is used, only the number of ports is displayed.

```
switch:admin> switchShow
switchName:     sw5
switchType:     2.1
switchState:    Online
switchRole:     Subordinate
switchDomain:   1
switchId:       fffc01
switchWwn:      10:00:00:60:69:00:00:0b
switchBeacon:   OFF
Zoning:         ON (c1)
port  0: sw 2G Online       F-Port 20:00:00:20:46:30:48:38
port  1: sw AN No_Light
port  2: sw 2G Online       F-Port 10:00:00:e0:69:00:02:b1
port  3: sw N2 In_Sync
port  4: -- AN No_Module
port  5: -- AN No_Module
port  6: cu 1G No_Light     L-Port
port  7: cu 1G Online       L-Port 8 private, 2 phantom
port  8: id AN No_Light
port  9: -- AN No_Module
port 10: -- AN No_Module
port 11: -- AN No_Module
port 12: sw AN No_Light
port 13: id 2G Online       E-Port (Trunk port, master is port #15)
port 14: -- AN No_Module
port 15: id 2G Online      E-Port 10:00:00:60:69:00:60:10 "sw6" (upstream)
(Trunk master)
```

To display the number of ports on the switch:

```
switch:admin> switchShow "-portcount"
ports=16
```

See Also

portcfgdefault

portcfgeport

portcfggport

portcfgislmode

portcfglongdistance

portcfglport

portcfgpersistentdisable

portcfgpersistentenable

portcfgshow

portcfgspeed
portcfgtrunkport
portdisable
portenable
switchdisable
switchenable
switchname

switchstatusshow

Displays the overall status of the switch.

Syntax

```
switchstatusshow
```

Availability

All users

Description

Use this command to display the overall status of the switch (enclosure). The overall status is calculated based on the switch status policy. (See switchstatuspolicyshow.) In addition, users with a Fabric Watch license are able to display the list of unhealthy ports, if such ports exist. The contributors to switch health are:

- Power supplies
- Temperatures
- Fans
- WWN server (dual CP-systems only)
- Switch redundancy (dual CP-systems only with HA enabled)
- Blade status (bladed-systems only)
- Port status
- Faulty ports
- Missing SFPs

The overall status can be in one of the following:

- HealthyEvery contributor is healthy.
- MarginalOne or more contributors are in this status.
- DownOne or more contributors are in this status.

If the overall status is not healthy, the contributing factors are listed also. See switchstatuspolicyshow for the calculation of the overall status.

Operands

None

Example

To display the switch status:

```
swd_152:admin> switchstatusshow
Switch Health Report                    Report time: 07/22/2003 09:12:39 AM
Switch Name:    swd_152
IP address:     192.168.204.152
SwitchState:    HEALTHY
Duration:       00:31

Power supplies          HEALTHY
Temperature sensors     HEALTHY
Fans                    HEALTHY
Marginal ports          HEALTHY
Faulty ports            HEALTHY
Missing SFPs            HEALTHY

All ports are healthy
```

See Also

`switchstatuspolicyshow`

`switchstatuspolicyset`

tempshow

Displays temperature readings.

Syntax

`tempshow`

Availability

All users

Description

Use this command to display the current temperature readings from each temperature sensor located on the switch's main printed circuit board (PCB). The sensors are located approximately one in each corner, and one at the center of the PCB.

Operands

None

Example

To display the temperature readings:

```
switch:admin> tempShow
35   28   29  Centigrade
95   82   84  Fahrenheit
```

See Also

fanshow

psshow

userconfig

Displays, adds, deletes, changes, or recovers user accounts.

Syntax

`userconfig [--actions][arguments]`

Availability

All users

Description

Use this command to display, add, delete, change, or recover switch user accounts. You can create new login accounts to manage a switch. These accounts take on the permission or role of the default admin or user account. When the command completes, the account name and other attributes are saved persistently. On a platform supporting multiple domains, the affected accounts apply only to the switch domain from which the command was executed.

In Secure Fabric OS mode, the actions associated with this command to add, delete, change, or recover accounts are allowed only on the primary FCS switch. The primary FCS switch distributes the update to the entire fabric. As a result, all switches supporting customer-defined accounts have the same account database. All accounts that are not consistent with the primary FCS switch are deleted and saved in the backup database. Administrators can use the `--recover` option to restore the accounts.

Operands

The command takes as input an action and its associated arguments. Without any specified action, the command displays the usage. Specify [*action*] as one of following:

`--show [`*options*`]` Displays current or backup account information.

`--add username [`*options*`]` Adds a new account, *username*, to the switch.

`--delete username` Deletes the account *username* from the switch.

`--change` *`username`* `[`*`options`*`]` Changes attributes for the account *`username`*.

`--recover [`*`options`*`]` Recovers one or more accounts from backup; created by Secure Fabric OS operations.

Note: The `--show` action is the only one available to accounts with user-level permission. All other actions require admin-level permission.

The following is a detailed description of each action type:

`--show [`*`username`*` | -a | -b]` Displays information about the current login account, the account named *`username`*, or all accounts either in the active or backup account database. If running from an account with user-level permission, it can display information only about itself.

`userconfig --show` Displays information about the current login account.

`userconfig --show` *`username`* Displays information about the account named *`username`*.

`userconfig --show -a` Displays information about all accounts.

`userconfig --show -b` Displays information about all accounts in the backup account database.

`--add` *`username`* `-r` *`rolename`* `[-d` *`description`*`]`

Adds a new account named username to the switch, with the given authorization of rolename. The `-d` option gives a text description for the new account. This command also prompts for an initial password. The following rules apply to add a new account:

— *`username`* must be unique and is case sensitive.

— *`username`* must begin with a letter and contain only letters, numerals, and underscores.

— The maximum length of *`username`* is 40 characters.

— *`description`* is optional; the maximum length is 40 displayable ASCII characters.

— *`rolename`* must be either user, admin, or nonfcsadmin. The nonfcsadmin role is applicable only in secure mode. In nonsecure mode, it is the same as admin.

There can be maximum 15 customer-created accounts for a switch.

`--delete` *`username`*

Deletes an existing account named *`username`* from the switch. This action does not accept any options. It prompts for the confirmation before proceeding. After an account is deleted, the CLI sessions associated with the account are terminated. An account cannot delete any default accounts or delete itself.

`--change` *`username`*
`[-r` *`rolename`*`]`
`[-d` *`description`*`] [-e yes | no]`

Changes attributes for an existing account, named *`username`*, in the switch. The `-r` option specifies a change to the authorization *`rolename`*. The `-d` option specifies a change to the description. The `-e` option accepts either yes or no to enable or disable an account. After an account is disabled, the CLI sessions associated with the account are terminated. The following rules apply:

— An account cannot change the *`rolename`* or *`description`* of any default accounts.

— An account cannot change the *`rolename`* or *`description`* for accounts at the same or higher authorization level.

— An account cannot change the *`rolename`* of itself.

Except the default root account, no account can disable itself.

`--recover`

Recovers all accounts from the backup database. After accounts were recovered, they are no longer present in the backup database. The backup database is created in Secure Fabric OS, when certain operations cause a switch to delete some of its customer-created accounts. For details, refer to the secure mode description.

Examples

To add a new account:

```
switch:admin> userConfig "--add joe  -r admin -d Joe Smith"
Enter new password:
Re-type new password:
Account joe has been successfully added.
```

To display current account information:

```
switch:admin> userConfig "--show joe"
Account name: joe
Role: admin
Description: Joe Smith
Enabled: Yes
```

To change account attributes:

```
switch:admin> userConfig "--change joe -e no"
Attribute for Account joe hsa been successfully changed.
```

zonecreate

Creates a zone.

Syntax

`zonecreate “zoneName”, “zoneMemberList”`

Availability

Admin

Description

Use this command to create a new zone; *zoneName* is a name for this new zone and cannot already be used for any other zone object; *zoneMemberList* is a semicolon-separated list of one or more:

- Physical fabric port numbers
- World Wide Names
- QuickLoop AL_PAs
- Zone alias names

A zone name is a C-style name (a name beginning with a letter and followed by letters, numerals, and underscore characters) up to 64 characters. Names are case sensitive; for example, `Zone_1` and `zone_1` are different zones. Spaces are ignored.

The zone member list has at least one member (empty lists are not allowed). The members are described by a semicolon-separated list of member definitions.

Physical fabric port numbers are specified as a pair of decimal numbers *s,p*, where *s* is the switch number (domain ID) and *p* is the port number on that switch; for example, `2,12` specifies port 12 on switch number 2. When a zone member is specified by physical fabric port number, all devices connected to that port are in the zone. If this port is an arbitrated loop, all devices on the loop are in the zone.

World Wide Names are specified as eight hexadecimal pairs separated by colons: for example, `10:00:00:60:69:00:00:8a`. Zoning has no knowledge of the fields within a World Wide Name; the eight bytes are simply compared with the node and port names presented by a device in a login frame (FLOGI or PLOGI). When a zone member is specified by node name, all ports on that device are in the zone. When a zone member is specified by port name, only that single device port is in the zone.

QuickLoop AL_PAs are specified as a QuickLoop name (referred to as a *qloop* name by zoning), followed by a list of AL_PAs: for example, `qloop1[01,02]`. QuickLoop names have the same format as zone names and are created with the `qloopcreate` command to define a switch or pair of switches that form the QuickLoop.

Zone alias names have the same format as zone names and are created with the `alicreate` command. The alias must resolve to a list of one or more physical fabric port numbers, World Wide Names, or QuickLoop AL_PAs.

The types of zone members used to define a zone might be mixed. For example, a zone defined with the members `2,12; 2,14; 10:00:00:60:69:00:00:8a` contains devices connected to switch 2, ports 12 and 14, and the device with a World Wide Name of `10:00:00:60:69:00:00:8a` (either node name or port name), whichever port in the fabric to which it is connected.

Note: This command changes the defined configuration (see `cfgshow`). For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

For the change to be preserved across switch reboots, it must be saved to nonvolatile memory using the `cfgsave` command.

When security is enabled, this command can be issued only from the primary FCS switch.

Operands

The following operands are required:

`zoneName`	A name for the zone, in quotes.
`zoneMemberList`	A semicolon-separated list of members, in quotes.

Example

To create three zones using a mixture of port numbers and zone aliases:

```
switch:admin> zoneCreate "Red_zone", "1,0; loop1"
switch:admin> zoneCreate "Blue_zone", "1,1; array1; 1,2; array2"
switch:admin> zoneCreate "Green_zone", "1,0; loop1; 1,2; array2"
```

See Also

`cfgtransabort`

`zoneadd`

`zonedelete`

`zoneremove`

`zoneshow`

zoneobjectcopy

Copies a zone object.

Syntax

`zoneobjectcopy "objectName", "newName”`

Availability

Admin

Description

Use this command to copy an existing zone object to a new zone object. The resulting object has the same type as the original object. You can use this command for all zone object types, including CFG, zone, and alias.

A zone configuration name must begin with a letter and can be followed by any number of letters, numerals, and underscores. Names are case sensitive; for example, `Cfg_1` and `cfg_1` are different zone configurations. Spaces are ignored.

This command changes the defined configuration. For the change to be preserved across switch reboots, it must be saved to nonvolatile memory, using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled, using the `cfgenable` command.

See the `zonecreate` command for more information on name and member specifications.

Note: This command requires an Advanced Zoning license. When security is enabled, this command can be issued only from the primary FCS switch.

Operands

This command has the following required operands:

`objectName` The name of the object that you want to copy.

`newName` The name of the object that you want created.

Example

To create a configuration containing three zones:

```
switch:admin> cfgShow "*"
cfg:   USA_cfg    Red_zone; White_zone; Blue_zone

switch:admin> zoneObjectCopy "USA_cfg", "UK_cfg"

switch:admin> cfgShow "*"
cfg:   UK_cfg     Red_zone; White_zone; Blue_zone
cfg:   USA_cfg    Red_zone; White_zone; Blue_zone
```

See Also

`cfgadd`

`cfgclear`

`cfgdelete`

`cfgdisable`

`cfgenable`

`cfgremove`

`cfgsave`

`cfgshow`

`zoneobjectrename`

zoneobjectexpunge

Expunges a zone object.

Syntax

```
zoneobjectexpunge "objectName"
```

Availability

Admin

Description

Use this command to expunge a zone object. In addition to performing a simple delete, this command also removes the object from the member lists of all other objects. Afterward, this object is completely removed from the database. You can use this command for all zone object types, including CFG, zone, and alias.

This command changes the defined configuration. For the change to be preserved across switch reboots, it must be saved to nonvolatile memory, using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled, using the `cfgenable` command.

Note: This command requires an Advanced Zoning license. When security is enabled, this command can be issued only from the primary FCS switch.

Operand

This command has the following required operand:

`objectName`	The name of the object you want to expunge.

Example

To create a configuration containing three zones:

```
 switch:admin> cfgShow
           Defined configuration:
            cfg:   USA_cfg    Red_zone; White_zone; Blue_zone
            zone:  Blue_zone
                   1,1; array1; 1,2; array2
            zone:  Red_zone
                   1,0; loop1
            zone:  White_zone
                   1,3; 1,4
            alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
            alias: array2  21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
            alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

switch:admin> zoneObjectExpunge "White_zone"

switch:admin> cfgShow
           Defined configuration:
            cfg:   USA_cfg    Red_zone; Blue_zone
            zone:  Blue_zone
                   1,1; array1; 1,2; array2
            zone:  Red_zone
                   1,0; loop1
            alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
            alias: array2  21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
            alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df
```

See Also

cfgadd

cfgclear

cfgdelete

cfgdisable

cfgenable

cfgremove

cfgsave

cfgshow

zoneobjectcopy

zoneobjectrename

zoneobjectrename

Renames a zone object.

Syntax

```
zoneobjectrename "objectName", "newName"
```

Availability

Admin

Description

Use this command to rename a zone object. You can use this command for all zone object types, including CFG, zone, and alias.

A zone configuration name must begin with a letter and can be followed by any number of letters, numerals, and underscores. Names are case sensitive; for example, `Cfg_1` and `cfg_1` are different zone configurations. Spaces are ignored.

This command changes the defined configuration. For the change to be preserved across switch reboots, it must be saved to nonvolatile memory, using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled, using the `cfgenable` command.

See the `zonecreate` command for more information on name and member specifications.

Note: This command requires an Advanced Zoning license. When security is enabled, this command can be issued only from the primary FCS switch.

Operands

This command has the following required operands:

objectName	The name of the object that you want to rename.
newName	The new name of the object.

Example

To create a configuration containing three zones:

```
switch:admin> cfgShow "*"
cfg:   USA_cfg    Red_zone; White_zone; Blue_zone

switch:admin> zoneObjectRename "USA_cfg", "UK_cfg"

switch:admin> cfgShow "*"
cfg:   UK_cfg     Red_zone; White_zone; Blue_zone
```

See Also

`cfgadd`
`cfgclear`
`cfgdelete`
`cfgdisable`
`cfgenable`
`cfgremove`
`cfgsave`
`cfgshow`
`zoneobjectcopy`

Fabric Watch User Guide

9

This chapter contains updates to the *HP StorageWorks Fabric Watch Version 3.1.x/4.1.x User Guide*, part number AA-RTSGC-AA.

On page 26, following the section "Activating with Web Tools," add the following:

Fabric Watch Reports

You can run reporting commands in Fabric Watch to get instant access to switch information. Although the `switchshow` command provides basic switch information, Fabric Watch reports provide detailed information and enable you to track marginal or faulty ports that can affect throughput or switch performance.

You can run reports on the command line using a telnet session or by using Advanced Web Tools (if you have installed a Web Tools license). Both tools generate reports that contain the same information, but it is presented differently.

Switch Health Report

The switch health report summarizes the overall health of a switch at a particular instant. The report lists:

- Current health of each port, based on the currently configured policy settings.
- High-level state of the switch, as well as its power supplies, fans, and temperatures.
- All ports that are in an abnormal state.

The switch health report is available even without Fabric Watch, but for licensed Fabric Watch users, the marginal and faulty ports are included in the report. The following is an example of a switch health report.

On page 114, preceding the section "Environmental Class Messages" add the following information:

Fabric Watch Message Formats

The format of all Fabric Watch messages is changed to a standard format that includes a unique message number. Fabric Watch also assigns a severity level to each message to indicate the degree of severity.

Fabric Watch threshold messages contain the following standard elements:

```
severity, severity number, timestamp, message number, sequence number,
severity, customer-assigned switch name, component name, message text,
component state
```

The following is a Fabric Watch threshold message in the standard format:

```
FW-FWWARNING, 3, 2004/09/14-20:08:59, [FW-0003], 1, WARNING, bigfsl32,
Fabric Env Temperature 2 ABOVE, current: 40 C (faulty)
```

Fabric Watch switch status messages contain the following standard elements:

```
severity, severity number, timestamp, message number, sequence number,
severity, customer-assigned switch name, message text
```

Following is a Fabric Watch switch status message in the standard format:

```
WARNING FW-FWWARNING, 3, 2004/09/14-20:10:30, [FW-0040}, 5, WARNING,
bigfsl32, Switch status changed from HEALTHY/OK to DOWN/FAILED
```

Table 21 describes the elements that appear in Fabric Watch messages.

Table 21: Fabric Watch Message Elements

Format Element	Description
Severity (Fabric Watch generated)	The level of severity of the message. Severity levels are: ■ INFO: an informational message indicating that a nominal event has occurred. ■ WARNING: indicates that a non-catastrophic error has occurred.
Severity Number	A system-generated value that indicates the level of severity. Valid values are: ■ 4 indicates an INFO message. ■ 3 indicates a WARNING message.
Time Stamp	The system time (UTC) when the message was produced on the switch.
Message Number	A unique identification number that you can use to determine if corrective action is necessary. The message number is a concatenation of a two-character alphabetical subsystem abbreviation and a numeric message number.
Sequence Number	The order in which the message was produced.
Severity (system generated)	The level of severity of the message. Severity levels are: ■ INFO: an informational message indicating that a nominal event has occurred. ■ WARNING: indicates that a non-catastrophic error has occurred.
Customer Assigned Switch Name	The switch that produced the message.

Table 21: Fabric Watch Message Elements (Continued)

Format Element	Description
Component	The element relevant to the message.
Message Text	Textual message containing up to eight parameters.
Component State	When appropriate, Fabric Watch messages include the state of the component in question. The value is identified by a keyword and the entire expression is in parenthesis.

Filtering Fabric Watch Messages

Fabric Watch assigns a severity level to each message when it is produced. You can set a filter so that only messages of a particular severity level and above are sent to the system and error logs. For example, if the level is set to Warning, only Warning, Error, and Critical messages are displayed and logged. Filtered messages are not shown on the console.

To filter Fabric Watch messages, issue the `fwset --message` command, and specify an integer that corresponds to one of the following Fabric Watch severity levels:

- Debug - 5
- Info - 4
- Warning - 3
- Error - 2
- Critical - 1

To view the current filter level setting for Fabric Watch, issue the `fwshow --message` command.

Setting Up Severity Level Filters on SNMP

Using the `agtcfgset` command, you can specify a trap recipient severity level filter on SNMP. The trap severity level is associated with each trap recipient's IP address. After specifying the IP address, specify the severity level for an event. That IP address (and only that IP address) then receives notifications when the severity level for that event is reached or surpassed. You do receive notifications unless the error matches or surpasses the specified severity level.

The severity level values for the traps are:

- None - 0
- Debug - 5
- Info - 4
- Warning - 3
- Error - 2
- Critical - 1

Note: When you specify a severity level filter on SNMP, it applies to Fabric Watch messages as well, so both SNMP and Fabric Watch messages are filtered.

```
Switch1_216:root> switchstatusshow
Switch Health Report                        Report time: 09/17/2004 9:03:01 PM
Switch Name:    Switch1_216
IP address:     10.32.170.61
SwitchState:    MARGINAL
Duration:       119:53

Power supplies monitor         MARGINAL
Temperatures monitor           HEALTHY
Fans monitor                   HEALTHY
Marginal ports monitor         HEALTHY
Faulty ports monitor           HEALTHY
Missing SFPs monitor           HEALTHY


All ports are healthy
value=0
Switch1_216:root>
```

Figure 33: Switch Health Report

The final portion of the report, detailing port health, is not available without a Fabric Watch license.

Port Detail Report

If the switch health report shows marginal throughput or decreased performance, use the port detail report to see statistics about each port. The port detail report conveys the overall health of one port, or a set of ports, at the time it is run. For each port, the port detail report lists the current state of health and all measurements contributing to that state. The port detail report is a Fabric Watch licensed product.

Figure 34 shows an example of a port detail report. An X in the column for a condition indicates that the condition has exceeded the threshold; a hyphen (-) indicates that the measurement is within range.

```
>fwportdetailshow
Port Detail Report                          Report time: 01/16/2004 11:12:28 AM
Switch Name:    swd21
IP address:     10.32.243.21
Port Exception report [by All]

                             --------Port-Errors------------ -----SFP-Errors----
Port# Type  State   Dur(H:M) LFA LSY LSI PER INW CRC PSC STM SRX STX SCU SV0
--------------------------------------------------------------------------------
000    E   HEALTHY   062:11   -   -   -   -   -   -   -   -   -   -   -   -
001    L   HEALTHY   062:11   -   -   -   -   -   -   -   -   -   -   -   -
002    E   MARGINAL  062:11   -   -   -   -   -   -   -   X   -   -   -   -
003    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
004    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
005    E   MARGINAL  062:11   -   -   -   X   -   -   -   -   -   -   -   -
006    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
007    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
008    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
009    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
010    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
011    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
012    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
013    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
014    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
015    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
016    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -
```

Figure 34: Port Detail Report

Table 22 lists and describes each category in the port detail report.

Table 22: Port Detail Report Columns

Report Item	Description
LFA	Link loss: the number of link loss occurrences out of range for the time period
LSY	Sync loss: the number of sync loss occurrences out of range for the time period
LSI	Signal loss: the number of signal loss occurrences out of range for the time period
PER	Protocol error: the number of protocol errors out of range for the time period
INW	Invalid word: The number of invalid words out of range for the time period
CRC	Invalid CRC: the number of CRC errors out of range for the time period
PSC	Port hardware state changed too often due to fabric reconfiguration
STM	SFP temperature is out of specifications
SRX	SFP receive power is out of specifications
STX	SFP transmit power is out of specifications
SCU	SFP current is out of specifications
SVO	SFP voltage is out of specifications

You can also use the `portshow` command to view the port health that Fabric Watch maintains. Valid port states are Healthy, Marginal, Faulty, and Offline.

Port Error Persistence

Port states indicate the overall health of a switch. While a port is operating, Fabric Watch monitors run every six seconds, gathering measurements about the port and looking for any abnormal behavior. When a value goes out of range, the monitor triggers.

Whenever a monitored value deviates from a user-defined range, the state of the port changes from a healthy state to an abnormal state. A port must remain in the abnormal state for a user-defined period of time before the port state affects the overall switch state. The monitor returns to a normal state when a problem is temporary. However, if the problem persists for 18 seconds or more, the state of the port changes from Healthy to Marginal. The port state remains Marginal as long as the problem exists.

You can modify the default error persistence value of `18`. To configure the port error persistence time, issue the `fwset --port --persistence` command.

index